Wireless Pers Commun (2013) 71:2259–2294
DOI 10.1007/s11277-012-0935-5

A Survey on Near Field Communication (NFC) Technology

Vedat Coskun · Busra Ozdenizci · Kerem Ok

Published online: 1 December 2012

Abstract Near Field Communication (NFC) as a promising short range wireless communication technology facilitates mobile phone usage of billions of people throughout the world that offers diverse services ranging from payment and loyalty applications to access keys for offices and houses. Eventually NFC technology integrates all such services into one single mobile phone. NFC technology has emerged lately, and consequently not much academic source is available yet. On the contrary, due to its promising business case options, there will be an increasing amount of work to be studied in the very close future. This paper presents the concept of NFC technology in a holistic approach with different perspectives, including communication essentials with standards, ecosystem and business issues, applications, and security issues. Open research areas and further recommended studies in terms of academic and business point of view are also explored and discussed at the end of each major subject's subsection. This comprehensive survey will be a valuable guide for researchers and academicians as well as for business world interested in NFC technology.

Keywords Near field communication · NFC · Survey · Communication essentials · Ecosystem · Business · Security · Applications · Application development · Secure element

1 Introduction

Ubiquitous computing and most recently ambient intelligence are defined as "technology becomes invisible, embedded, and is enabled by simple interactions, attuned to all our senses and adaptive to users and contexts" [14]. Nowadays, technology has been invisibly embedded into daily objects and they are becoming more and more ubiquitous. The increasing mobility of computing devices provided by mobile communications becomes an important step in the development of ubiquitous computing.

V. Coskun · B. Ozdenizci (✉) · K. Ok
Isik University, Istanbul, Turkey
e-mail: busraozdenizci@isikun.edu.tr

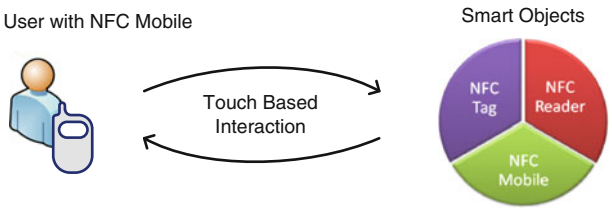

Fig. 1 Touch based paradigm for NFC

Mobile phones had already several communication options with the external environments before the introduction of Near Field Communication (NFC) technology. When the mobile phones were initially introduced, the primary goal was to enable voice communication with the mobile and wired phones. GSM (Global System for Mobile Communications) communication enabled functionality of mobile phones for several services, such as voice communication, SMS (Short Messaging Service), MMS (Multimedia Messaging Service) and even Internet access. Bluetooth technology was introduced later 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. This interaction can be identified as "the deliberate bringing together of two devices, for the purpose of obtaining services" [17]. NFC as one of the enablers for ubiquitous computing is a "combination of contactless identification and interconnection technologies" [95] which requires bringing two NFC compatible devices close to each other, essentially touching them. In accordance with [36], user first interacts with a smart object (either an NFC tag, NFC reader, or another NFC enabled mobile phone) using her NFC enabled mobile phone (in short: NFC mobile). After touching occurs, NFC mobile may further make use of received data, or may alternatively use provided mobile services such as opening a web page, making a web service connection etc. (Fig. 1).

Up to now, many NFC trials are conducted over the world, especially in payment domain. All trials conclude the fact that with the development of NFC technology, mobile phone is subject to become safer, more convenient, speedier and more fashionable physical instrument. NFC technology allows people to integrate their daily-use loyalty cards, credit cards etc. into their mobile phones. In addition to integrating those cards into mobile devices, NFC technology brings innovation opportunities to mobile communications. It enables two users to easily communicate and exchange data simply by touching two mobile phones to each other. Moreover NFC technology gives NFC reader capability to mobile phones; hence RFID (Radio Frequency Identification) tags can be read.

An encouraging property of NFC technology is the assurance of secure storage of the personal and private information on the secure element of the mobile phones those are traditionally saved in other items such as credit or debit cards. Due to the technical enforcement of touching paradigm, it is harder to tap the data since the mobile communication is performed within a short distance.

With the increasing processing power of mobile phones, Internet access capability, and many more features; innovative services are enabled by NFC technology. It is true that NFC technology brings simplicity to transactions, provides easy content delivery and enables information sharing. At the same time, it builds new opportunities for various stake holders; mobile operators, banks, transport operators and merchants with faster transactions, less cash handlings and new operator services.

This study presents the concept of NFC technology in a holistic approach with different perspectives; communication essentials, ecosystem and business issues, applications and security issues; and also provides a comprehensive survey with open research areas and guidelines.

The remainder of this paper is organized based on the major research areas of NFC technology. In Sect. 2, we present the communication essentials related with the NFC technology including operating modes and protocol stack architectures, NFC devices and hardware issues, and finally data transmission properties on Radio Frequency (RF) layer. In Sect. 3, the security and privacy issues regarding NFC technology is discussed. The exploration of Secure Element (SE) and its management are discussed in Sect. 4. In Sect. 5, the potential service domains of NFC technology are presented which show NFC technology's increasing popularity by academicians, researchers and practitioners. Furthermore, at the end of each major section we provide useful guidelines, and recommend open research issues for the reader.

2 Near Field Communication Technology

NFC technology was jointly developed by Philips and Sony in late 2002 for contactless communications [127]. It is a short-range half duplex communication protocol, which provides easy and secure communication between various devices (Table 1). In accordance with [94], NFC is distinct from far field RF communication that is used in personal area and longer-range wireless networks. NFC relies on inductive coupling between transmitting and receiving devices. The communication occurs between two compatible devices within few centimeters with 13.56 MHz operating frequency [36,89,105,127].

The acting two parts of NFC communication is categorized as initiator and target devices [27]. The Initiator is the device that initiates and guides the data exchange process between the parties. The target is the device that responds to the requests made by the initiator. According to Cho et al. [34], NFC protocol distinguishes between two modes of operation, which are active mode and passive mode. In the active communication mode both devices uses their

Table 1 Comparison of WPAN technologies [25,88]

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 MHz
Security	Low	Low	High
Network topology	Piconets, scatternets	Star, tree, mesh	One to one
Devices per network	8	2–65,000	2
Usability	Moderate, data centric	Easy, data centric	Easy, human centric
Personalization	Medium	Low	High
Flexibility	High	High	High
Setup time	Approx. 6 s	Approx. 0.5 s	Less than 0.1 s

Table 2 Active versus passive communication mode [71]

Device A	Device B	RF field generation	Communication mode
Active	Active	Generated by both devices	Active mode
Active	Passive	Generated by Device A only	Passive mode
Passive	Active	Generated by Device B only	Passive mode

Table 3 Interaction styles of NFC devices

Initiator device	Target device
NFC mobile	NFC tag
NFC mobile	NFC mobile
NFC reader	NFC mobile

own energy to generate their own RF field to transmit the data. In the passive communication mode only initiator generates the RF field while the target device makes use of the energy that is created by the active device (Table 2).

There exist three NFC devices, which can involve in NFC communication: NFC mobile, NFC tag, and NFC reader. Table 3 shows the possible interaction styles among those NFC devices. NFC technology operates in three different operating modes: reader/writer, peer-to-peer, and card emulation modes where communication occurs between an NFC mobile on one side, and an NFC tag, an NFC mobile, and an NFC reader on the other side respectively [100,127]. Each operating mode uses distinct communication interfaces (i.e. ISO/IEC 14443, FeliCa, NFCIP-1, NFCIP-2 interfaces) on RF layer as well as has different technical, operational and design requirements [41,44,127].

In accordance with [36,100,127], the RF interface supports communication with data rates of 106, 212 as well as 424 kbps as of today. As mentioned in [36,162], NFC uses different modulation schemes such as ASK (Amplitude Shift Keying) with different modulation depth—100 or 10 %—or load modulation and coding techniques such as NRZ-L (Non-Return-to-Zero Level), Manchester and Modified Miller coding to transfer data. In each NFC transaction, the NFC communication mode of an initiator or target NFC devices (active or passive), the signaling 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 that is used. The study [smart] shows the summary of techniques used in NFC transaction depending on the direction of the communication. ISO/IEC 18092 (NFCIP-1) is the combination of ISO/IEC 14443 Type A and JIS X 6319 Type F. The study [64] deals with the increase of data rates for proximity coupling devices at 13.56 MHz and NFC systems, and compares performance of ASK and PSK modulation schemes in a real environment. It shows that PSK performs 23 % better in terms of field strength requirement and energy efficiency than ASK (Fig. 2).

2.1 NFC Mobile Architecture

NFC technology integrated (NFC enabled) mobile devices are typically composed of various integrated circuits, such as a secure element (SE) and an NFC communication interface as depicted in Fig. 3. NFC interface is composed of a contactless, analogue/digital front-end

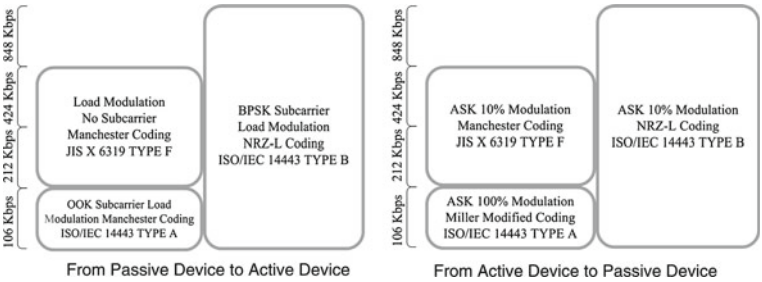

Fig. 2 Modulation and coding schemes

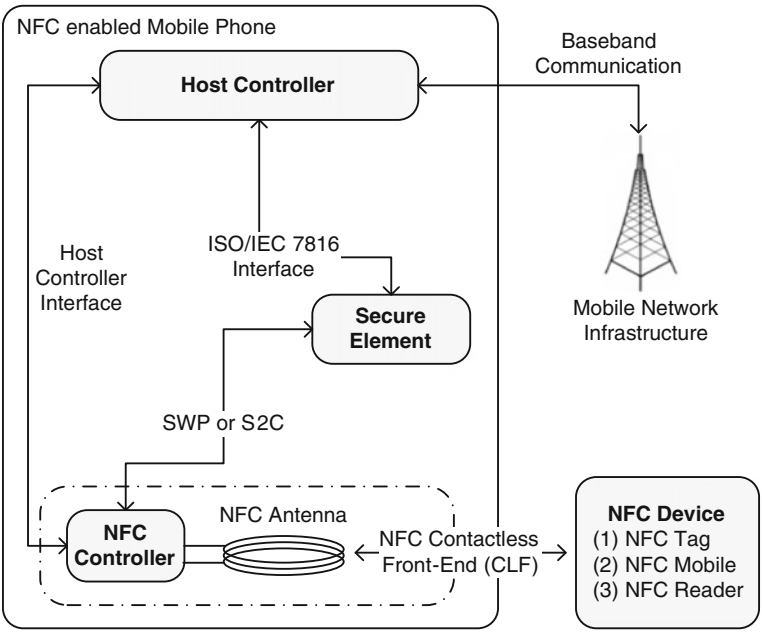

Fig. 3 General architecture of NFC enabled mobile phones

called as NFC Contactless Front-end (NFC CLF), an integrated circuit called as NFC controller to enable NFC transactions, and an NFC antenna.

The study of Gebhart and Szoncso [58] describes the antenna design methods in combination with transponder system properties to show how to efficiently combine established chip platforms with smaller antenna form factors. Similarly, in literature, other novel proposals and experimental approaches can be found on optimizing the design of NFC antenna for readers and transponders [22,31,32,35,114,169], and also on the design of NFC transceiver chipset [35,113,146] for improving the communication quality, RF interface and security.

An NFC enabled mobile phone consists of secure element(s) for performing secure transactions using NFC devices as well as storing sensitive data in a secure environment. In accordance with [3,60,61,143], secure element provides a dynamic and secure environment for both programs and data. It enables storage of valuable, sensitive, and private data such as credit card information of the user, and secure storage and execution of NFC enabled services such as contactless payments, which is valid in card emulation operating mode.

The mobile device may contain additional SEs based on the requirements. NFC controller is connected to SEs through either Single Wire Protocol (SWP) [47] or NFC Wired Interface (NFC-WI) [42]. However NFC literature does not include any comparison analysis of both physical layers in terms of security, performance or other parameters yet.

The SE can be accessed and controlled from host controller (internally) as well as from RF field (externally). The host controller, or baseband controller in other words, is the heart of the NFC mobile. Host Controller Interface (HCI) creates a bridge between the NFC controller and the host controller [48]. The host controller sets the operating modes of the NFC controller through HCI, processes data that is sent and received, and establishes the connection between the NFC controller and the secure element.

2.2 NFC Operating Modes and Their Essentials

NFC technology benefits from various elements such as smart cards, mobile phones, card readers, and payment systems. In accordance with [36], all of the proposed candidates need to acquire accreditation from an assortment of governing bodies that have the responsibility for controlling security and interoperability of NFC devices. Various standardization bodies defined how the NFC technology should be integrated to mobile phones and other related devices. Some other bodies defined the architectures and standards for the security issues as well as the ancillary technologies for NFC enabled mobile phones such as smart cards for NFC transactions. The common vision of all standardization bodies is increasing the ease of access, interoperability, and security for NFC technology.

The most important association that focuses on developing and improving the use of short-range wireless interaction through NFC technology is NFC Forum [127]. It is a non-profit industry association that was established with the aim of enabling NFC technology at first, and making it spread around the world thereafter. The mission of NFC Forum is to promote the usage of NFC technology by developing specifications, ensuring interoperability among devices and services, and educating the market about NFC technology. Up to now NFC Forum provided diverse specifications for the various components of NFC technology such as LLCP (Logical Link Control Protocol) [124], NFC Tag Types [125], NFC RTDs (Record Type Definitions) [120–123,126] and so on. Hence NFC literature does not include high amount of research issues in terms of communication essentials; thus some experimental and performance testing studies can be conducted.

The three NFC communication modes are defined based on which NFC device is paired and performing communication with NFC mobile. The communication protocols, standards, etc. differs for each operating mode.

2.2.1 Reader/Writer Mode Communication Essentials

In reader/writer operating mode, active NFC mobile initiates the wireless communication, and can both read and modify the data stored in NFC tags. NFC tags are actually passive RFID tags, which can be also referred as NFC transponders [58,93,103]. In this operating mode, NFC mobile is capable of reading NFC Forum mandated tag types, which are Type 1, Type 2, Type 3 and Type 4 [125]. This enables mobile user to retrieve the data stored in the tag and take appropriate action afterwards (Fig. 4).

In addition to NFC forum mandated tag types, NFC Forum has standardized data exchange format (i.e., NFC Data Exchange Format, NDEF) between communication parties. NDEF defines the format of the data to be exchanged between two NFC devices [119]; between active NFC device and passive tag, or active NFC device and active NFC device.

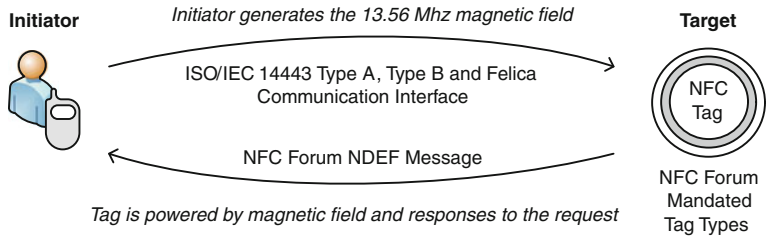

Fig. 4 Reader/writer operating mode

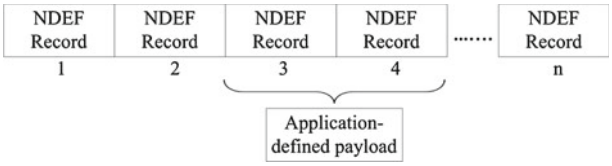

Fig. 5 NDEF message with a set of records

According to NFC Forum [119], NDEF is a binary message format that encapsulates one or more application defined payloads into a single message as depicted in Fig. 5. Roland and Langer [144] defines NDEF as a standardized format for storing formatted data on NFC tags and for transporting data across a peer-to-peer NFC link.

An NDEF message contains one or more NDEF records. Records can be chained together to support even larger payloads. A record is the unit for carrying a payload within an NDEF message. Each NDEF record carries parameters for describing its payload; payload length, payload type, and an optional payload identifier. NDEF records are variable length records with a common format illustrated in Fig. 6. Each individual field in a record has different features [119,120]. The record layout is explained below:

- MB (Message Begin): The MB flag is a 1-bit field which indicates the start of an NDEF message.
- ME (Message End): The ME flag is a 1-bit field which indicates the end of an NDEF message.
- CF (Chunk Flag): The CF flag is a 1-bit field which indicates that this is either the first record chunk or a middle record chunk of a chunked payload.
- SR (Short Record): The SR flag is a 1-bit field which indicates that the PAYLOAD_LENGTH field is a single octet.
- IL: The IL flag is a 1-bit field which indicates that the ID_LENGTH field is present in the header as a single octet.
- TNF (Type Name Format): The TNF field value represents the structure of the value of the TYPE field. The TNF field is a 3-bit field with values defined in the Table 4:
- TYPE_LENGTH: This field is an unsigned 8-bit integer that specifies the length in octets of the TYPE field. The TYPE_LENGTH field is always zero for certain values of the TNF field.
- ID_LENGTH: This field is an unsigned 8-bit integer that specifies the length in octets of the ID field.
- PAYLOAD_LENGTH: This field is an unsigned integer that specifies the length in octets of the PAYLOAD field (the application payload). The size of the PAYLOAD_LENGTH field is determined by the value of the SR flag.

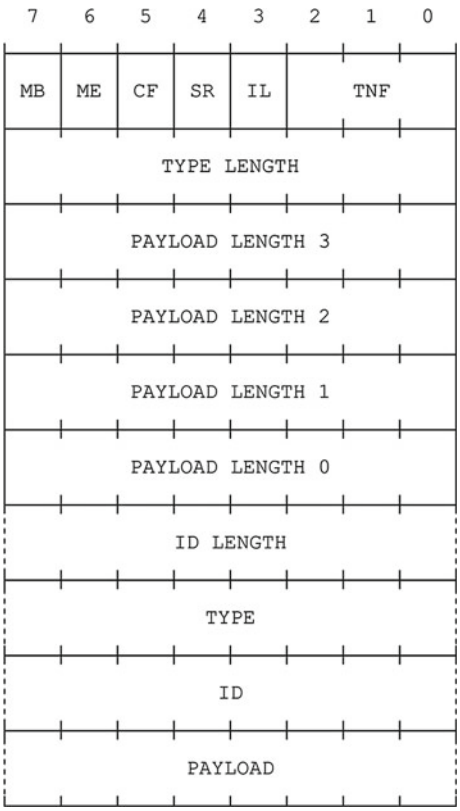

Fig. 6 NDEF record format [119]

- TYPE: This field describes the type of the payload.
- ID: The value of the ID field is an identifier in the form of a URI reference.
- PAYLOAD: This field carries the payload intended for the NDEF user application.

Various record types for NDEF messaging format are defined by NFC Forum [120–123,126]. 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 (Uniform Resource Identifiers), NFC Forum external type names or well-known NFC type names [119,120,127]. Each record type definition is identified by its record type name.

2.2.1.1 Protocol Stack Architecture for Reader/Writer Operating Mode

Figure 7 provides a useful protocol stack illustration for reader/writer mode [127]. The NFC device operating in reader/writer mode has the following protocol stack elements:

- Analogue and digital protocols are the lower protocols in physical layer section. Analogue is related with RF characteristics of NFC devices and determines the operating range of devices. Digital protocols refer to the digital aspects of ISO/IEC 18092 and ISO/IEC 14443 standards, and define building blocks of communication. There is also another important specification by NFC Forum at this level which is NFC Activities Specification. This specification defines the required activities that set up communica-

Table 4 Type name format (TNF) field values [119]

Type name format	Value
Empty	0×00
NFC Forum well-known type	0×01
Media-type	0×02
Absolute URI	0×03
NFC Forum external type	0×04
Unknown	0×05
Unchanged	0×06
Reserved	0×07

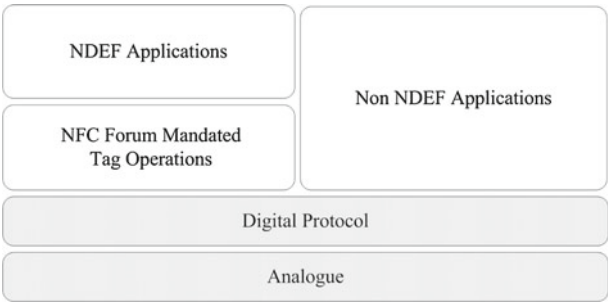

Fig. 7 Protocol stack of reader/writer operating mode

tion in an interoperable manner based on digital protocol specification such as polling cycles, when to perform collision detection.

- Tag operations indicate the commands and instructions used by NFC devices to operate NFC Forum mandated tags which are Type 1, Type 2, Type 3, and Type 4. They enable read and write operations by using the NDEF data format and RTDs (i.e. Smart poster, URI RTDs) from/to a tag.
- NDEF applications are based on NDEF specifications such as smart poster applications and reading product information from NFC enabled smart shopping fliers.
- Non NDEF applications are vendor specific applications which are not based on NDEF specifications such as electronic purse balance reader and contactless ticket reader.

2.2.2 Peer-to-Peer Mode Communication Essentials

In peer-to-peer mode, two NFC mobiles establish a bidirectional connection to exchange information as depicted in Fig. 8. Peer-to-peer operating mode's RF communication interface is standardized by ISO/IEC 18092 as NFCIP-1, which enables "request-response model" between two active devices [38,58,65]. In this mode, NFC mobiles can exchange any kind of data such as business cards, digital photos, and so on.

According to the study [162], NFCIP-1 protocol provides a SAR (Segmentation and Reassembly) Level 1 capability, as well as data flow control depending on the Go and Wait principle usual for half duplex protocols. Furthermore, NFCIP-1 protocol allows error handling by using accept (ACK) frame and reject (NACK) frame, provides an ordered data flow, and performs the communication in the link layer which is reliable and error free [162].

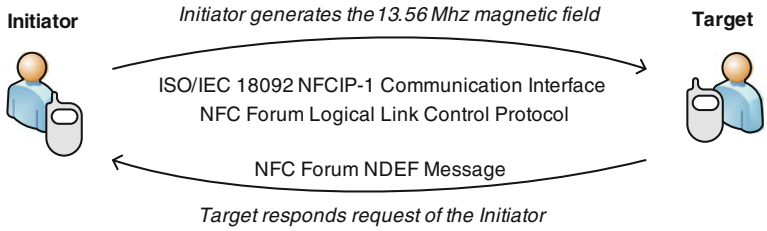

Fig. 8 Peer-to-peer operating mode

The study in [2] presents a simulation model for the NFCIP-1 over the network simulator. The study indicates that NFCIP-1 protocol needs to be supported with other techniques such as flow control mechanisms; hence the proposed model is a good starting point for many research issues.

A new data link layer protocol, named as LLCP, is standardized by NFC Forum [65,124] to support peer-to-peer communication between two NFC enabled devices. LLCP is essential for any NFC application that performs bi-directional communication. LLCP provides a solid ground for peer-to-peer mode applications and enhances the basic functionalities provided by NFCIP-1 protocol as well. According to NFC Forum [124], LLCP provides five important services; connectionless transport; connection-oriented transport; link activation, supervision and deactivation; asynchronous balanced communication, and protocol multiplexing.

NFCIP-1 takes the advantage of initiator-target paradigm in which the initiator and target devices are defined prior to starting the communication. However the devices are identical in LLCP communication. After the initial handshake, the decision is made by the application that is running in the application layer. In study [67], a valuable comparison is performed between NFCIP-1 and LLCP through a social networking application. Both NFCIP-1 and LLCP were tested during the application development. Since LLCP does not define which device will be the initiator, the user can easily experience in MAKING friends with LLCP. An extended investigation of LLCP with a simulation model is a promising research area as well.

2.2.2.1 Protocol Stack Architecture for Peer-to-Peer Operating Mode

Similarly according to the NFC Forum Specifications [127], an NFC device operating peer-to-peer mode has the following protocol stack elements as depicted Fig. 9:

- Analogue and digital protocols are lower layer protocols standardized by NFCIP-1.
- LLCP allows transferring upper layer information units between two NFC devices. Protocol bindings provide standard bindings to NFC Forum protocols and allow interoperable use of registered protocols.
- NFC Forum protocols are the ones that NFC Forum defines a binding to LLCP, such as OBEX, IP.
- Simple NDEF exchange protocol allows exchange of NDEF messages. It is also possible to run other protocols over the data link layer provided by LLCP.
- Applications may run over the simple NDEF exchange protocol, other protocols or NFC Forum protocols. These applications are such as printing from a camera, business card exchange etc.

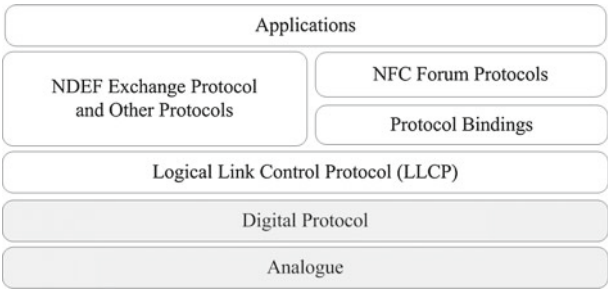

Fig. 9 Protocol stack of peer-to-peer operating mode

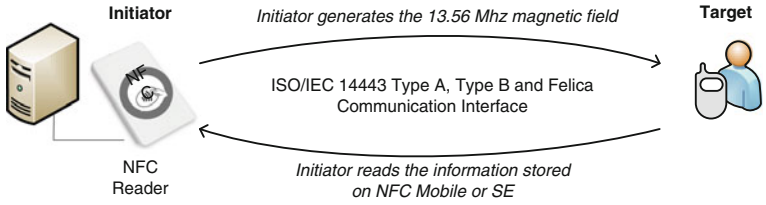

Fig. 10 Card emulation operating mode

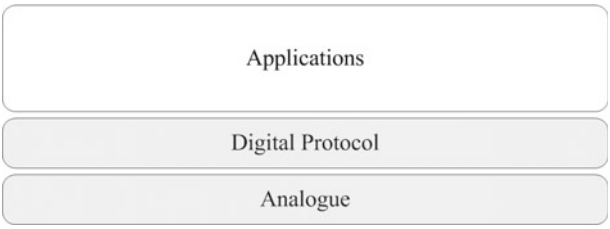

Fig. 11 Protocol stack of card emulation operating mode

2.2.3 Card Emulation Mode Communication Essentials

In card emulation mode, NFC devices use similar digital protocol and analogue techniques with smart cards and they are completely compatible with the smart card standards based on ISO/IEC 14443 Type A, Type B and FeliCa [100,127]. As the user touches her mobile phone to an NFC reader, NFC mobile behaves like a standard smart card, thus NFC reader interacts with the applications on the SE. Only card emulation mode uses an SE efficiently and securely, which performs functions that require high security (Fig. 10).

2.2.3.1 Protocol Stack Architecture for Card Emulation Operating Mode

NFC devices those are operating in card emulation mode use similar digital protocol and analogue techniques with smart cards and they are completely compatible with the smart card standards (Fig. 11). Card emulation mode includes proprietary contactless card applications such as payment, ticketing and access control [127]. These applications are based on ISO/IEC 14443 Type A, Type B and FeliCa communication interfaces.

2.3 Open Research Issues

There are some other open research areas that should be improved more by academicians and researchers. Some of the challenging studies on network, hardware as well as software levels are listed below.

- Development of alternative protocols for NFC additional to NFCIP-1, LLCP for promoting P2P transactions,
- Development of simulation modules for NFC protocols such as NFCIP-1,
- Analysis of antenna coupling, RF efficiency, ferrite quality and cost saving issues,
- Development of simulation models for NFC tags as transponders,
- Design of new modulation and coding techniques for NFC,
- Exploration of simple and low-power modulation schemes,
- Design of optimized high bandwidth policy,
- Analysis of power saving and power consumption issues,
- Proposal of manageable NFC functionality and user interfaces on NFC mobiles in hardware as well as software aspect,
- Examination of NFC Dynamic Tags which enables dynamic data, rather than NFC Static Tags,
- Integration of NFC technology with OS,
- Development of Quality of Service mechanisms in NFC context.

3 Secure Element and Its Management

In accordance with [49], since NFC technology enables various contactless ticketing, payment, and other similar applications, storing and managing valuable and private information (e.g. credit card, debit information) in the secure area of the NFC mobile is a requirement for NFC based systems. If not, the data could be transmitted via a GSM or other interface to a third party who may misuse them. To solve such activities, relevant NFC applications need to be executed and saved in a protected environment, which is the memory of a secure element (SE) of NFC mobile. SE is combination of hardware, software, interfaces, and protocols embedded in a mobile handset that enables secure storage. The SE has also an operating system (e.g., MULTOS, JavaCard) that supports the secure execution of applications and the secure storage of application data.

Up to now various SE alternatives entered into 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 [36,110,143], mainly SE options can be grouped under removable SEs, non-removable SEs, software based SEs on dedicated hardware, and other flexible SE solutions. Figure 12 shows the currently available SE options for each SE category. Understanding the characteristics of SEs plays significant role for different stakeholders and pricing models in the NFC value chain. The dominating SE will have a strong position to build trusted services on it.

- **Embedded SE:** Embedded SE is a smart card that is integrated to the mobile phone, which cannot be removed. According to the study [143], the level of security provided by this SE is as high as the one supported by a smart card. This chip is embedded into the mobile phone during manufacturing process and must be personalized after the device is delivered to the end user [143].

- **Sticker:** According to Mobey Forum [110], NFC sticker's aim is to allow service providers a quick way to launch pilots and start to deploy NFC services such as payment, loyalty, transportation, and so on. Two types of stickers are available; active and passive stickers. In theory, active stickers enable all NFC services and give NFC functionality to non-NFC mobiles. Also life cycle management of active stickers is possible because of their connection with the mobile phones. They are mainly developed to give NFC functionality to mobile phones, however when NFC mobile phones are spread all over the world, their usage is decreased. There is not much practical implementation of NFC services management with stickers [110].
- **SMC:** Secure memory card (SMC) provides same high-level security as a smart card provides, and it is compliant with most of the main standards and interfaces of smart cards (e.g. GlobalPlatform, ISO/IEC 7816, JavaCard etc.). As mentioned in [143], with the removable property and a large capacity memory, an SMC can host high number of applications in it. Currently, most of the trials are performed on SMCs.
- **UICC:** UICC is a generic multi-application platform for smart card applications where SIM or USIM is implemented upon. UICC provides an ideal environment for NFC applications that are personal, secure, portable and easily managed remotely via OTA technology [3,60,61]. It can host non-telecom applications from various service providers such as loyalty, ticketing, healthcare, access control, and ID applications [110]. GlobalPlatform provides the most promising standard for UICC life cycle management (or namely card content management) with three different business models; simple as MNO centric model, delegated model and full authorized as TSM centric model [3,60,61]. However, there are still some unsolved issues on UICC card management in NFC based services. Hence there is not any UICC smart card commercially available in the NFC market [110].
- **Flexible SE Solutions:** In early years of NFC, because of lack of NFC mobiles in the market, several alternative architectures have been proposed to enable NFC to the mobiles without integrated NFC capability. Especially SMC and SIM based SEs with built-in NFC antennas has acted as an important NFC bridge devices (e.g., SMC hosting only NFC antenna and SE, or hosting NFC chip, antenna and SE and so on) [36]. They shorten the time-to-market contactless payment and similar applications. The study of [98] proposes an alternative that integrates NFC with SIM card; SIM Application Toolkit.
- **TMB:** Trusted Mobile Base (TMB) is a promising upcoming technology that is proposed by Mobey Forum. It is hosted at the root of the mobile phones and defined as a secure isolated section on the Core Processor Units (CPU) of mobile phones [110]. Various secure NFC enabled applications can be provided flexibly via OTA technology. According to [110], TMB has the full potential of becoming a SE in the future.

3.1 Over-the-Air (OTA) Technology

Over-the-Air (OTA) technology contributes dynamic spirit of the NFC based system adaptability to flexible environments [3,102]. It enables loading and installation of new NFC applications on SEs - especially on UICCs - remotely, activation and deactivation of SEs, remote service management, life-cycle management of NFC applications on the SEs, and other online services. High-capacity bearers those are being used in OTA technology are very important in providing an NFC solution [158]. For instance, several kilobytes of data needs to be transferred to the UICC based SE when downloading

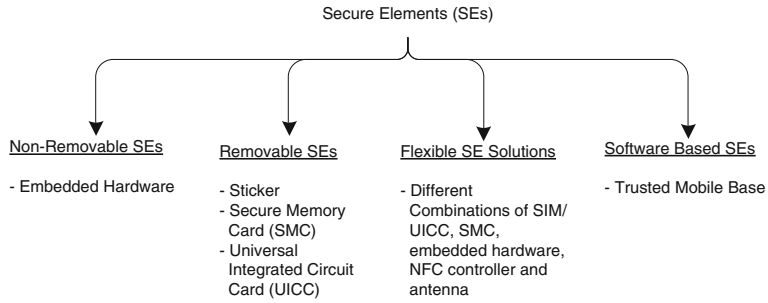

Fig. 12 Summary of SE alternatives

an application activation data or an NFC application. Using GPRS/UMTS and the BIP (Bearer Independent Protocol) protocol, applications are rapidly deployed OTA to the UICC card.

Currently, most MNOs are capable of providing OTA solutions using their current technology infrastructure. However, it is also possible to see that when required infrastructure is set up by other entities, these entities can provide OTA service independently from SE issuers or platform managers. One of the most appropriate cases is to use OTA solution of Trusted Service Manager as a neutral entity within the NFC ecosystem.

The studies [97,100,102] outline an infrastructure concept for setting up a sustainable NFC ecosystem and introduce new concept as platform manager. According to them, platform provider can be identified also as a Trusted Service Manager (TSM) and is the key enabler for OTA transactions which acts as a middleman between service providers and secure elements within NFC mobiles [36]. At the same time the initialization and personalization of the SEs, the role of platform provider and outgo/income of each stakeholder in this business model is analyzed. The major challenge is that the proposed process involves several different components and instances, which indeed makes the standardization process difficult. There is high amount of uncertified components within NFC ecosystem; hence there is no proven security for the OTA transactions.

The proposed model [102] is a beneficial model for the NFC applications that require OTA transactions. This model can also be studied on smart card web server (SCWS) applets. However it can be further improved for protecting integrity and confidentiality of the keys and personal data on SE and avoiding other possible risks.

3.2 Life Cycle Management of SE

The life cycle management of an SE within NFC mobile starts after the issuance of SE to the user, which covers first process as installation and personalization, and the next process as remote management process. Rigorous studies on the life cycle management of SEs are somewhat missing due to the lack of standardization in processes. A study [3] examines the feasibility of loading, installation, and personalization process of a payment application on UICC based SEs using the GlobalPlatform specifications. The experimentation results reveal that the functional roles and actors in a delegated management business model need to be further examined; since the delegated model requires partnerships of each service provider with each card issuer, and the complexity might occur in application management. For other SE options, appropriate models need to be developed as well.

Another important issue is hosting multiple SEs in an NFC mobile, which needs further consideration. For example, a mobile phone may contain embedded hardware, or SMC, together with a UICC. GlobalPlatform performed valuable analysis on the potential implications of managing multiple SEs in the same mobile handset. They provided two business models for managing multiple SEs in a single mobile handset as with aggregation and without aggregation business models [62]. Madlmayr et al. [99] provides a fruitful proposal for secure management of multiple SE called Secure Element Controller (SEC). SEC internally controls the communication flow; routes the data streams to the appropriate SE chip, and handles SE's authentication. Moreover, with the analysis of security and interoperability, it has been observed that this model has several benefits for NFC based systems. The model can be also practically implemented and improved with all SE alternatives instead of only removable ones.

3.3 Open Research Issues

There are still various open research issues such as the ideal SE option, standardization processes of SE life cycle management process, and so on. To sum up, some critical research issues are identified in this research area that can be examined, improved, and evaluated by academicians as well as practitioners:

- Verification of existing tools within the market such as GlobalPlatform,
- Applicability verification of multi-application SE platform management (up to now performed trials usually include one service. However users would prefer a dynamic NFC environment including more than one service when necessary),
- Implementation of multiple SEs support within single mobile,
- Exploration of MNOs' existence in pre-installation and personalization of NFC applications, whether it creates security related problems or not,
- Comparison of bearer alternatives in OTA downloading and personalization processes in terms of security, data transmission, and other issues,
- Clarification of key management and key rotation issues, especially for each SE alternatives when loading and installing applications,
- Analysis of life-cycle management perspective of SIM Application Toolkit.

4 NFC Security and Privacy

As same with all information systems, NFC based systems are subject to attacks those threaten system security and user privacy. As described in [78,79], we need to consider that if NFC services are managing our private information, then the applications of these NFC services and the system interaction must be reliable and safe. In NFC attacks, the target can be entire NFC system or it may be the just the NFC component (e.g., tag, reader, mobile, backend) of the NFC system. Someone attacking an NFC system or an NFC device may desire to place misinformation to an NFC mobile phone or to an NFC tag. According to the study of Madlmayr et al. [101], the major assets that need to be protected within NFC based systems are:

- The user's privacy which is represented by the data stored on the host controller of NFC mobile such as short messages as well as information on the SE such as tickets;
- NFC functionality and operability of the device;
- Functionality of the host controller and applications on SE;
- Information exchanged between NFC devices over the RF link;

- Information stored on NFC tag.

In terms of standardization, only NFCIP-1 protocol's security is standardized so far which focuses on the information exchange between two NFC mobiles, i.e., peer-to-peer operating mode. On top of NFCIP-1, NFC-SEC (NFCIP-1 Security Services and Protocol) standard is promoted to provide security capabilities to it and consists of two different protocols [43]. Therefore, applications using peer-to-peer mode do not require application specific encryption mechanisms for the security services those are provided by NFC components. Actually it is highly necessary to see more NFC specific cryptography standards for services operating in different modes.

4.1 Security Analysis of Data on NFC Tags

Actually these attacks have high importance for reader/writer mode applications since NFC tags are the major components of those applications, which provide valuable data for users. Actually, an attacker can easily manipulate the data stored on the tag using different activities such as replace or hide original tag on a smart poster with a malicious tag, break the write protection of the tag and overwrite it with malicious data, clone or impersonate those tags and so on.

Several vulnerability testing methods are performed in [115] by analyzing NDEF record structure, smart posters, and URI handling through fuzzing tests; and identified some important attacks on NFC tags. The major attacks described in [115,163] are infecting NFC mobiles through NFC worms or worm-URL, which are hidden in a smart poster tag, some spoofing attacks, as well as DOS attacks which can also frustrate the relationship between customer and service provider.

Attackers can spoof the tag content, which means that attacker supplies false information such as a fake domain name, false e-mail etc., that looks valid and the system accepts by mistake. Smart poster URI spoofing is one of the best examples of spoofing in terms of NFC [115]. The smart poster URI spoofing further allows for attacks against web browsers, URLs as well as attacks against mobile telephony services using SMS URIs, telephony URI, and so on. Mulliner aims to improve the fuzzing process through automation and also develop more efficient methods for analyzing the vulnerabilities since NFC devices are becoming more complex in future work.

It is possible for an attacker to create a malicious poster with modified NDEF tags by altering an existing commercial poster [115,144,145] that leads malicious content sharing with attacker. To handle attacks on NFC tags, trustworthiness of the tags on a smart poster by signing them with appropriate encryption techniques is essential. One solution is to use signatures in NDEF messages as mentioned in [126,144]. The study of [Roland] examines the NFC Forum's Signature Record Type Definition (RTD) to enable adding digital signatures to the NDEF message for protecting the data integrity as well as enabling authentication. However in another study [144,145], signature record type's vulnerabilities have been discovered and analyzed, and also some basic guidelines to avoid the risk of such attacks are outlined. According to the results, signature record type records needs development for enabling security of NDEF record within a tag.

4.2 Security on Readers

As mentioned earlier, NFC reader is an important NFC device, which mainly enables card emulation mode applications consisting of an NFC enabled mobile phone on one side and

a reader on the other side. However, there is not any sufficient study on the security of NFC readers and countermeasures in the literature so far. Furthermore, since NFC readers are nearly the same with RFID readers, NFC readers can also be subject to destruction or removal [109]. NFC readers can be stolen especially when they are situated in unattended places. An NFC reader can contain critical information such as cryptographic keys, which can be the target of an attacker. Attackers can reach sensitive information similar within tag impersonation process.

4.3 Security on Radio Frequency Interface

Since NFC is a wireless communication interface, it is obvious that variety of attacks can be possible when two NFC devices communicate using RF waves. Actually being a short-range communication is an advantage for securing NFC communication, however in some cases this is not a strict limitation for the attacker. The study of [78,79,88,154] performs review of the possible attacks on RF interface of NFC and suggests some prevention mechanisms and protocols for those attacks. The most discussed attacks are eavesdropping, DOS (Denial-of-Service) attacks, MIM (Man-in-the-Middle) attacks, relay attacks [53], and phishing by social engineering.

The most comprehensive and rigorous analysis is performed in [71] where several attacks and their countermeasures are assessed with technical details and use cases. In addition to the mentioned attacks, the study also evaluates the data insertion and modification attacks as well. The study suggested that the feasibility of the presented attacks highly depends on the applied strength of the amplitude modulation. Only solution to protect NFC especially from eavesdropping is establishing a secure channel between NFC devices with a shared secret between two NFC devices; such as using a standard key agreement protocol (e.g., Diffie-Hellman based on RSA -Ron Rivest, Adi Shamir and Leonard Adleman-, Elliptic Curve Cryptograph) or an NFC specific key agreement protocols proposed in [71]. For the MIM attack it is indicated that in real world this attack is practically infeasible since in case of an active device communicating with a passive device, the perfect alignment of RF field of active device and attacker's RF field is impossible.

In another study [101], the security aspect of NFC technology is examined through communication interfaces, component and trust levels within NFC system. They have proposed some mechanisms to protect those interfaces and some of these proposals also have similarities with the ones proposed in [78,79]. Some of the interesting ones are introducing a button to turn on NFC functionality consciously by the user for avoiding relay attacks, introducing a management instance for the SEs in the device, using signed tags to prevent phishing attacks and so on.

According to Madlmayr et al. [101], some of the security and privacy issues can also be solved by technical means and standardization on NFC devices, which is an important research area. Also testing platforms for analyzing the security of RF interface are missing in the literature; generally use case approach has been observed.

4.4 NFC Mobile and SE Security

Another important part of the NFC based systems is the security of NFC mobile and its SE. In a related study [101], an assessment on the importance of NFC mobile and SE security is performed. If SE security is not considered; applications on the host controller may run without the knowledge of the user, or malware applications may be installed on host controller

or SE that can make use of other data stored on the device, processes may be initialized by the NFC controller, or OTA management of SE may be eavesdropped, or an attacker may add a modified SE to the NFC mobile and make use of security leaks. Hence, some certificate-based authentication mechanisms beside the strength of OS running on the host controller and SE are required that needs attention of the researchers and academics.

The valuable studies in [52,54] analyze the skimming and token cloning attack on NFC mobiles with embedded SE by performing a practical implementation. A number of security countermeasures (e.g., control measures on NFC SE, mandatory code signing for NFC communication API, linking applications to Unique Identifiers cryptographically) are proposed to prevent such a misuse. However in another study [97], this issue is directly associated with the smart cards, not NFC technology. For other SE options, these attacks and their feasibility need to be experimented and addressed with effective security countermeasures.

In another valuable work on SEs [84], an authentication system based on SIM authentication is presented. It is stated that the SIM's potential in secure storage of keys enables mobile phone to act as a highly advanced authentication device. With the proposed key management in [84], it is able to provide a security management for any service access. Different key management policies can be examined for enabling authentication and integrity as well. Table 5 provides a brief summary of all possible security attacks, vulnerabilities of NFC based systems and their solutions according to the academic studies.

4.5 Open Research Areas

In terms of technical point of view, security issues in NFC technology are not completely solved and standardized yet and this actually causes literature to be immature. Up to now, among a number of proposals, only a small percent of the papers provides valuable insights on the security issues of NFC technology with implementations and reliable analysis.

It has been observed that most of the published papers provide application-specific cryptographic algorithms, protocols, secure platforms and key management mechanisms with evaluation methods or testing results, such as [28–30,33,51,63,167]. They generally solve only one or few security services (i.e., authentication, data integrity and so on) and answer specific problems. Appropriate authentication mechanism in financial transactions is an important research area since NFC has high potential in financial service domain. Relating with these studies, following future studies are identified which will be a helpful guide for the academicians interested in security issues of NFC:

- Development of alternative NFC specific security and privacy mechanisms,
- Development of security mechanisms for protecting NDEF records within a tag,
- Proposal of authentication algorithms for signing NFC tags and NFC applications,
- Exploration of vulnerabilities of NFC readers,
- Exploration of securing SE activity and enabling control measures on SE,
- Experimental comparison of SE alternatives in terms of vulnerability,
- Development of prevention mechanisms and protocols for the vulnerabilities in management of each SE option,
- Proposal of countermeasures for relay attacks, implementation of location proofs for NFC applications on mobiles,
- Design of optimized NFC antennas for overcoming the RF interface attacks,
- Exploration of middleware and backend systems' security especially for card emulation mode applications,
- Study of alternative digital certificate management and certificate authorities,

Table 5 Vulnerabilities, attacks and solutions

Vulnerabilities and attacks	Solutions
NFC tags	
Tag manipulation (infecting NFC mobiles through NFC worms, URI spoofing, URL spoofing, phone call spoofing, SMS spoofing, DOS attacks etc.)	Signing tags appropriate encryption techniques
Tag clonning and tag impersonation	Using cryptographic tag authentication protocols
Tag replacement and tag hiding	
RF interface	
Eavesdropping	Secure channel establishment between NFC devices
MIM attacks	NFC specific key agreement protocols
Data corruption	
Data modification	
Data insertion	
DOS attacks	
Relay attacks	
Phishing by social engineering	
NFC mobile and SE	
Running applications on host controller (without the knowledge of the user)	Certificate-based authentication mechanisms
Installation of malware applications on host controller or SE	Key management policies for authentication and integrity for SE control measures on NFC SE
Attacking NFC controller	Mandatory code signing for NFC communication API
Eavesdropping OTA management of SE	Adding modified SE to NFC mobile
Skimming and token cloning attacks	Linking applications to unique identifiers cryptographically

- Proposal of NFC specific alternative key agreement protocols and secure channel mechanisms to prevent eavesdropping attack besides standard key agreement mechanisms,
- Development of low cost, interoperable, high security frameworks and platforms; including proper cryptographic measures, signature and certificates, e.g., Elliptic Curve Cryptography (ECC) to increase the size of key rather than RSA solutions, compatibility of ECC with signature RTDs, integration of ECC with SEs etc.
- Development of simple and well structured testing and simulation tools for NFC security,
- Clarification of legal restrictions, policies and regulations in NFC context,
- Exploration of NFC in terms of privacy sensitivity and ethical issues.

5 NFC Ecosystem

From the ecosystem point of view [36], NFC industry has a new emerging business environment opportunities and large value chain including several industries and organizations such as mobile network operators, banking and payment services, semiconductor producers and

electronic appliances, software developers, other merchants including transport operators and retailers. The potential business opportunities of NFC technology 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 on the fact that NFC services to end users cannot be provided by a single firm. From the technical point of view, the standardization of NFC technology has already started [11]. However NFC take-off has been slower than expected. In [97,100], it is mentioned that the use cases for the end customer are clear but the structure of the ecosystem as well as its value chain is not set yet. The main reason of this slow take-off is highly 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.

In [7–10], the deficiencies of NFC based solutions collaborating with existing contactless and smart card standards are explored in a comprehensive approach. In accordance with these studies, the problems within the NFC ecosystem can be identified as follows:

– Technological and operational problems:
  - Currently mobile NFC applications are handset specific. Hence, service providers and mobile operators have to develop and maintain a unique application for each NFC device model.
  - Although NFC technology warrants the separation of various applications on the same chip with very high security and minimal risk of interference; some certain security specifications prohibit this coexistence. Thus, the management of multiple applications on the same chip is also an unsolved issue.
  - OTA service provisioning is a great benefit of mobile technology. However, diverse technical OTA solutions exist and these are not interoperable with each other [9]. As also discussed in [110], "Today's OTA solutions have capacity limits. When entering new environments with more sophisticated banking applications, the current OTA solutions do not have sufficient enrolment capacity to provide the required security, power, duration and usability."
  - Currently, different technical infrastructures of secure elements (SEs) for different NFC enabled services exist; hence each actor proposes a model that brings more advantage to that actor than others. For example MNO's propose SIM based models, since they can control the UICC cards and hence can receive more profit if this model is used.

– Managerial and strategic problems:
  - The revenue to be shared is enormous and this creates failure in common understanding and vision in working with suitable and necessary business models in NFC ecosystem.
  - Participating organizations to the ecosystem are powerful in their own industry, so that they all think that the other parties must follow their needs.

To achieve a good business model; interoperability, compatibility and standardization of the accepted NFC technology model are essential. It is also important to drive cooperation of partners in the ecosystem and also to enable customer acceptance. Currently there is a tremendous amount of work on organizing the contributions and interests of all entities, and better governance of the overall ecosystem. From the technical point of view, to create

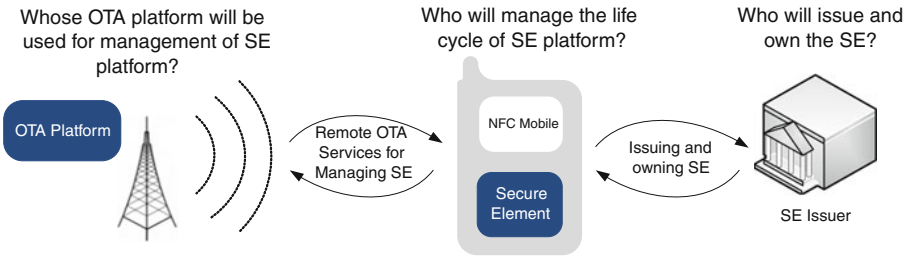

Fig. 13 Creating business model

sustainable business models for NFC services, some issues need to be completely solved from all involving parties' aspects (Fig. 13). Three main issues (i.e., secure element issuer, platform manager and OTA provider) generally determine and structure business model for an NFC service currently. These issues can also be referred as functional roles and responsibilities that need to be handled by a single entity or multiple entities in NFC business model.

In addition to this approach, a good methodology for sustaining NFC business models is provided in [82]. This study explores NFC mobile ticketing business models holistically and identifies critical issues that affect the commercial success of NFC ticketing service. It utilizes a theoretical framework called as STOF (Service, Technology, Organization and Finance) model, which offers a good analytic tool for identifying the critical issues related to diverse participants within NFC mobile ticketing ecosystem. The framework focuses on four interrelated domains as service, technology, organization, and finance to create a holistic view in evaluating business models; hence it helps to create value for both customers and other players within ecosystem.

Another study in [7] explains a technically transparent and uniform platform called "host application" for managing multiple services dynamically on an NFC mobile, irrespective of the handset type or manufacturer. This provides also well-structured methodology to identify the commercial dependencies, problems within ecosystem, and to distribute risks between key stakeholders. Actually practical implementation of such business model proposals is missing in the literature. The literature review performed in [135] also indicates that approximately 9.46 % of the NFC literature focuses on NFC ecosystem and business issues. Business models of the NFC technology need to be clearly considered with methodologies and design principles that have theoretical proofing.

5.1 Open Research Issues

Some challenging research areas related with the NFC ecosystem that should be examined are listed below.

- Development of sustainable ecosystem model for NFC services including revenue-cost analysis, SE usage, competency and feasibility analysis,
- Exploration of economic performance of NFC based systems,
- Examination of proposed NFC applications' business impacts and models based on some theoretical frameworks in a holistic approach like in study [x],
- Business analysis of complex NFC applications such as NFC based transportation and NFC payment systems,
- Validation and test of new business model solutions,

- Exploration of business case opportunities based on demography, regulation, market structure, and infrastructure readiness etc.,
- Identification of liability issues, customer care, and division of other related roles and responsibilities between the key stakeholders,
- Standardization and certification of OTA infrastructure and platform, security mechanisms, NFC applications and so on; the certification of this chain of components is vital in order to establish an NFC ecosystem,
- Standardization and certification of SEs and their life cycle management; common security criteria for SE is highly essential for deployment of NFC services,
- Comparison and evaluation of SE issuing process of MNOs and other providers, and OTA processes in different geographical regions.

6 NFC Applications

Since NFC technology is started to be promoted, various real-life applications have been evolved. An NFC literature review study in [135] revealed that, about 40 % of the NFC literature concentrated on developing new NFC applications. Indeed, design artifacts, which propose composed applications or services operating in two or more modes can be seen in NFC literature [134].

6.1 Review on NFC Applications and Service Domains

6.1.1 Healthcare Applications

In the last decades, one of the fields where IT is playing fundamental role is healthcare. Providing effective and appropriate healthcare services is one of the most important objectives of information and communication technologies. It is seen from the literature that NFC plays significant role in health service domain due to its easy use with lower consumption property. NFC provides user-friendly remote health monitoring, controlling, and tracking systems [13,15,16,18,50,74,104,132,161], and electronic data capturing services [111,112,140]. There are also some services that aim to improve the care dependent people's quality of life such as NFC enabled prescription system [164], storage of encrypted medical data on tags [40], adverse drugs reaction and allergy detection systems in pharmaceutical and medical care [77,80].

6.1.2 Smart Environment Applications

In technological perspective, smart environment is defined in [149] as "a physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements and also embedded seamlessly in the everyday objects of our lives, and connected through a continuous network". NFC technology can be also buried in applications that address diverse and heterogeneous needs and capabilities of users in the real world, and make users' life easier.

Most of the smart environments are enabled by NFC tags that are distributed around. In accordance with [75], "tags can provide support in user's everyday life activities by establishing a bridge between the physical and 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".

It is possible to see innovative examples of smart environment in the NFC literature, which makes use of NFC tags to simplify utilization of existing functions of a system [160], to control a system and perform services remotely [24,75,139,149–151,155] and also to provide information channel [1,12,19,23,68,69,91,147,153]. N-CASH is another example for NFC enabled smart environment [25,26] that clearly describes the creation of a smart space, which can be activated by NFC mobile to control devices such as home appliances. The appliances are controlled and driven by the request from NFC mobile that uses predefined ontology and rule based reasoning. So, NFC mobile acts as the key to enter the space as well as provide personalized control of a variety of appliances in that space.

6.1.3 Data Exchange and Sharing Applications

The exchange of data, image, or similar content between two NFC mobile is also another important application domain provided by NFC technology. Especially today, between potential business partners, exchanging contact data is really important for continuity of the relationship in business world. The proposed system, named VisiExchange prototype [38], enables mobile devices to share data by peer-to-peer operating mode and eliminates the risk of unwanted data transfer with third parties.

6.1.4 Mobile Payment, Ticketing and Loyalty Applications

With the market and technological developments, successful mobile payment solutions have already been launched over the world. Actually some countries are much more advanced in terms of deployed technology and implemented business cases since governments and influential mobile network operators (MNOs) in those countries have powerful impact on enhancing the development of mobile payment services [131]. Various technologies contributed for the development of mobile payment systems such as RFID technology, contactless smart cards, Short Message Service (SMS), USSD (Unstructured Supplementary Service Data (USSD), WAP (Wireless Application Protocol) IVR (Interactive Voice Response) and so on.

Currently, integration of NFC technology with mobile payment systems brought new and innovative business solutions. Payment, ticketing and loyalty applications are possibly the most well-known and promising everyday applications of NFC technology and have the most complexity in ecosystem aspect as well. Thus it can be seen that most of the trials and projects (e.g., Payez Mobile Project [138], Pay-Buy-Mobile Project [66], SIESTA Project [5]) are implemented in this application domain. Some of these projects still continue with growing participating entities. From the academic point of view, some valuable studies have been performed as well as some fruitful usability and user experience analyses in payment and payment related application domains. Some examples are:

- An automated reservation and ticketing service for tourists, and a system for car parking access and payment system for ticketing [5,6],
- Virtual ticketing system and secure mCoupon protocol [1,39,73],
- Secure payment service by Smart Touch Project [137],
- NFC Ticketing system with a simple architecture, including usability testing [59],
- NFC Loyal system including a secure data exchange model to promote payment and loyalty applications on secure elements [133],
- Offline Tapango system for electronic ticketing process including comparison with traditional paper ticketing process [117],

- Offline NFC payment service with electronic vouchers [37],
- Secure payment system built on a Service Oriented Architecture (SOA) including payment authorization process [83].

6.1.5 Entertainment Applications

Although NFC technology has high potential for applications like payment and ticketing, applying NFC technology in entertainment and social media applications is receiving more and more attention on user side. Some examples from the literature are Pass the Bomb and Exquisite Touch games [116] which are implemented with a multi-player purpose; Whack-a-Mole game [20,21] which combines dynamic NFC displays to explore mobile interaction with tagged, physical objects can leverage mobile gaming; PhonePhone as an NFC enabled musical instrument [76].

6.1.6 Social Network Applications

Currently, Internet based social network applications are booming with popular services like Facebook, LinkedIn, MySpace and Twitter etc. NFC technology is also an enabler for social networking tools and can be integrated with the existing social network applications [67,70,90,156]. Generally, these applications enable users to interact with tagged physical objects and publish information with the virtual world. Some trials are also using peer-to-peer mode to allow users to share and access their personal information, to create friendships in a more tangible and user friendly way [56,67,156]. Another good way of promoting social network services is to provide also advertising and location based services such as TaggyNet [4].

6.1.7 Educational Service Applications

Currently, universities and schools became a valuable research area for development and testing NFC technology. Various implementations of NFC services and prototypes in universities can be seen to create smart environments for the students as well as to perform efficient work force management and easier administration services for the staff. Up to now, diverse innovative NFC services in university settings are tested and implemented [106–108,148] such as identification, payment services in university cafes and restaurants, photocopy services, reservation and payment of sports facilities, and also resources control and management services, teaching services, dissemination of information and accessing to services.

Also NFC technology can be used in interactive learning process of students [57,152]. For example, the proposed Moodle system in [57] enables use of games in teaching and learning process. It brings together the characteristics of a common strategy game with an evaluation system; and enables to motivate and reward students by using NFC mobiles. Other valuable examples related with the efficient work force management in school settings are NFC enabled attendance supervision system [45,46], and examination systems supported by NFC technology in universities [159].

6.1.8 Location Based Applications

Location based services (LBSs) are used for enabling an information service by using the geographical position of the user's mobile device. With the integration of LBSs with NFC

Table 6 Benefits and underlying values of NFC applications

Reader/writer mode	Peer-to-peer mode	Card emulation mode
Increases mobility	Easy data exchange	Physical object elimination
Decreases physical effort	Device pairing	Access control
Ability to be adapted by many scenarios		
Easy to implement		

technology, users' behavior can be tracked and user experiences can be improved [72,136]. Depending on the position of the user, most common examples are displaying friends nearby, broadcasting advertisement of stores nearby through SMS/MMS, and discovering nearest post office depending on our geographical position. Hence these services provide location based, customized messages or information to users [72,92,157]. Such services can also be integrated with NFC enabled the indoor navigation systems [76,136] to provide more value added services to the users, especially in shopping centers.

6.1.9 Work Force and Retail Management Applications

Furthermore NFC technology contributes in solving the problems within the business world and work force management. For example, in retail industry, retailers face various problems in sales data management such as high cost, low security, and poor performance of real-time documentation [86,142,168]. Nowadays, it is possible to see the advantages of NFC technology in improving the existing business processes within companies [85,87,96,118, 130,166].

6.2 Evaluation of NFC Applications

Each NFC application provides different benefits and underlying values for its user. The study in [128,129] performed valuable review of literature and exploration of NFC services' benefits. The benefits of those services can be examined by classifying them into their operating modes. The communication essentials are different in each operating mode, and these differences make change in benefits and usage areas. Table 6 provides the summary of NFC applications' benefits in terms of their operating modes.

6.3 Exploring User Experiences in NFC Applications

According to the resources [127], the NFC simplifies the human environment interaction and enables users only to wave their mobile devices in front of everyday objects augmented with RFID tags in order to trigger intelligent services, which makes NFC easy to use. By this way a user can access services, set up connections, make payment, or use a ticket. Up to now, when we look at the literature, it is seen that only few studies [55,81,130,165] have performed well structured usability analysis on NFC to measure the success of trials and user experience.

An academic work for a subjective usability study of a student council voting is studied in [130] which compares NFC mobile voting with web based voting scenario. NFC voting gained a higher usability than web based voting with a score of 82.75 whereas web

based voting gained a score of 78.50 out of 100. The results of the usability test showed that NFC technology has the potential to increase the usability of systems. As a result, the rise of NFC compatible mobile phones and services will bring new opportunities to make our lives easier. In the context of voting, NFC provided a practical and easy to use environment.

Another study in [81] also performed usability tests on NFC to identify how NFC based systems could be used to improve mobile solution work flows and usability. The study showed that NFC can improve mobile workflows by solving different related problems. In the pilot cases, NFC technology dealt with the problems of access to real-time information, applications and instructions in the field, real time updating of data, removal of human errors, reducing users' memory payload and so on. The study concluded that NFC based solutions are easy to use, but the small and limited keyboard of mobile devices causes difficulties for the design of the models. NFC based solutions should take into account the place of the tags, ease of the application usage, and the amount of textual input. The study showed that user friendliness was taken into account in the pilots, but it did not always impact on the user experience.

6.4 Challenges and Factors Influencing Design of NFC Based Systems

Several costs may affect the design and development of NFC based systems directly or indirectly. In many academic studies, NFC technology seems to have a cost cutting affect, however financial and economic side of NFC application and system development are not considered in a clear way for practitioners and system developers. Relating with [141], some important factors influencing the design of NFC based systems and applications have been explored as follows:

- Cost of the NFC tag, tag placement and management,
- Cost of the NFC readers and reader placement,
- Cost of training and reorganization,
- Cost of developing NFC applications,
- SE Programming and management,
- System integration costs,
- Cost of OTA processes,
- Testing costs of the NFC systems and applications,
- Maintenance costs of overall systems.

6.5 Developing NFC Applications

Developing NFC applications is an important part of NFC technology. In order to develop NFC applications, complete understanding of NFC technology and operating modes are required. There are two different types of applications in NFC services; Graphical User Interface (GUI) application and SE application. GUI application exists in all operating mode applications and provides an interface, which allows a user to interact with the mobile device. It also provides the capability to read/write from/to NFC components. On the other hand, SE applications are needed in order to provide a secure and trusted environment for security required applications (e.g., payment, loyalty, ticketing).

There are various development tools on the market targeting different mobile phones. Some of these development tools are Android SDK (Software Development Kit) for Android

mobile phones; Qt SDK for Symbianˆ3 mobile phones; Bada SDK for Bada operating system phones and Series 40 Nokia 6212 NFC SDK for Nokia 6212 devices. Each development tool has a unique SDK and uses different language. The developer who wants to develop application on a specific platform needs to know that platform's programming language and NFC APIs (Application Programming Interfaces) built for that platform. Fortunately, today operating principles of different platforms' NFC APIs are similar to each other. Hence the developers can easily work and develop NFC applications on different platforms.These SDKs provide Reader/Writer mode and Peer-to-Peer mode programming.

However, in order to develop card emulation mode applications, the SE (i.e. UICC card) needs to be programmed using Java Card programming language. NFC reader communicates with the Java Card applet in the SE to perform transactions in this case. In addition, in order to develop a mobile application that communicates with the SE (i.e. displaying the transactions performed in the SE) you may also code another mobile application with the corresponding SDK (i.e. Android SDK).

6.6 Open Research Issues

We believe that future research effort is needed in this area as well. Up to now, various NFC trials, projects and prototypes have been done; however some of them give us valuable insights about the technology's development, usability, adoption, and acceptance issues. Due to the slowness of standardization efforts, some practitioners do not answer completely their research questions and complete their research with the expected goals. For example, there are still some unsolved issues in card emulation mode and SE programming which create different and propriety NFC solutions, incompatibility of applications as well as restricts the interoperability of different platforms. Some research areas are listed as follows:

- Development of novel NFC applications those will help growth of NFC ecosystem,
- Comparison of vulnerabilities of NFC applications in different domains,
- Comparison of alternative ubiquitous wireless services with NFC and a review study based on this work,
- Exploration of co-existence NFC applications on the same SE,
- Analysis of compatibility and interoperability of different NFC mobile architectures for running applications using NDEF message exchange,
- Exploration of tag management, placement, and maintenance,
- Operational and strategic study on integration of NFC based components and related issues into a larger system such as number of tags to be placed, required training, and skilled employees,
- Methodology development for smart posters including visual symbols as NFC tags,
- Proposal of multiple OS support for NFC environment,
- Integration of seamless web services with NFC applications,
- Proposal of alternative application development environments based on needs,
- Exposure of software development methodologies for NFC applications,
- Development of design principles, methodologies and models for building specific applications such as context aware or smart environment,
- Creation of user interaction models for different application domains,
- Exploration of user perception and preferences for NFC systems,
- Identification of barriers to and critical success factors for NFC adoption,

- Exploration of different cultures and cultural norms impact on NFC usability case studies,
- Exposure of psychological and relational issues in NFC adoption,
- Implementation of longitudinal field studies on NFC usability with well structured statistical results,
- Analysis of security and privacy issues impact on adoption and acceptance of NFC technology. security
- Clarification patent issues in NFC based systems.

7 Conclusion

In recent years, NFC has become an attractive research area for many researchers and practitioners due to its exploding growth and its promising applications and related services. The number of publications in NFC research area is increasing continuously since 2005 [135]. With this study, we provide a comprehensive survey on NFC technology and its ecosystem including review of all academic studies as well as some valuable white papers of industry pioneers within NFC ecosystem. Such as survey study is a beneficial way for understanding the current status of NFC research area.

Current academic studies on NFC are mainly published on conferences. In the contrary only a few journal publications exist. We have reviewed all such publications and referred the significant works in this survey. With this survey, we want to encourage more insight into the critical issues and problems of NFC technology, and facilitate providing solutions to the open research areas which are presented in this paper.

To sum up, there is a clear need especially for more journal publications to solve the issues that have mentioned in the open research problem sections. Academicians and researchers need to focus on these recommended research issues, and give publications that have high level of research both in width and breadth [134,135] to maintain the advancement of knowledge in NFC research and to identify the gap between theory and practice.

References

1. Aigner, M., Dominikus S., & Feldhofer, M. (2007). A system of secure virtual coupons using NFC technology. In *Proceedings of fifth annual IEEE international conference on pervasive computing and communications workshops*, pp. 362–366.
2. Ali, W., El Kilani, W., & Hadhoud, M. (2010). Simulation of NFCIP-1 protocol over NS-2. In *Proceedings of 7th international conference on informatics and systems*, Cairo, Egypt, pp. 1–6.
3. Alimi, V., & Pasquet, M. (2009). Post-distribution provisioning and personalization of a payment application on a UICC based secure element. In *Proceedings of international conference on availability, reliability and security*, Fukuoka, pp. 701–705.
4. Aziza, H. (2010). NFC Technology in mobile phone next-generation services. In *Proceedings of the 2nd international workshop on near field communication*, Monaco, pp. 21–26.
5. Baldo, D., Benelli, G., & Pozzebon, A. (2010). The SIESTA project: Near Field Communication, based applications for tourism. In *Proceedings of 7th international symposium on communication systems networks and digital signal processing*, Newcastle upon Tyne, pp. 721–725.
6. Benelli, G., & Pozzebon, A. (2010). An automated payment system for car parks based on near field communication technology. In *Proceedings of international conference for internet technology and secured transactions (ICITST)*, London, pp. 1–6.
7. Benyó, B., et al. (2009). The StoLPan view of the NFC ecosystem. In *Proceedings of the conference on wireless telecommunications symposium*, Prague, pp. 1–5.
8. Benyó, B. (2009). Business process analysis of NFC-based services. In *Proceedings of IEEE 7th international conference on computational cybernetics*, Palma de Mallorca, Spain, pp. 75–79.

9. Benyó, B., et al. (2007). NFC applications and business model of the ecosystem. In *Proceedings of 16th IST mobile and wireless communications summit*, Budapest, pp. 1–5.
10. Benyó, B., et al. (2007). The design of NFC based applications. In *Proceedings of 11th international conference on intelligent engineering systems*, Budapest, pp. 277–280.
11. Biader Ceipidor, U., et al. (2008) NFC: Integration between RFID and mobile, state of the art and future developments. In *Proceedings of emerging technologies for radio frequency identification*, pp. 78–81.
12. Blöckner, M., et al. (2009). Please touch the exhibits!: Using NFC-based interaction for exploring a museum. In *Proceedings of the 11th international conference on human–computer interaction with mobile devices and services*, Bonn, Germany.
13. Bravo, J., Hervas, R., Fuentes, C., Chavira, G., & Nava, S. W. (2008). Tagging for nursing care. In *Proceedings of second international conference on pervasive computing technologies for healthcare*, Tampere, pp. 305–307.
14. Bravo, J., et al. (2007). Touch-based interaction: An approach through NFC. In *Proceedings 3rd IET international conference on intelligent environments*, Ulm, pp. 440–446.
15. Bravo, J., et al. (2008). Enabling NFC technology for supporting chronic diseases: A proposal for Alzheimer caregivers. In *Proceedings of the European conference on ambient intelligence*, pp. 109–125.
16. Bravo, J., et al. (2008). Enabling NFC technology to support activities in an Alzheimer's day center. In *Proceedings of the 1st international conference on pervasive technologies related to assistive environments*, Athens, Greece.
17. Bravo, J., et al. (2008). From implicit to touching interaction: RFID and NFC approaches. In *Proceedings of conference on human system interactions*, Krakow, pp. 743–748.
18. Bravo, J., et al. (2008). Identification technologies to support Alzheimer contexts. In *Proceedings of the 1st international conference on pervasive technologies related to assistive environments*, Athens, Greece.
19. Bravo, J., et al. (2008). Towards natural interaction by enabling technologies: A near field communication approach. In *Proceedings of AmI 2007 workshops*, pp. 338–351.
20. Broll, G., et al. (2010). Touch to play—mobile gaming with dynamic, NFC-based physical user interfaces. In *Proceedings of the 12th international conference on human computer interaction with mobile devices and services*, Lisboa.
21. Broll, G., et al. (2011). Touch to play—exploring touch-based mobile interaction with public displays. In *Proceedings of 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 15–20.
22. Brown, T. W. C., & Diakos, T. (2011). On the design of NFC antennas for contactless payment applications. In *Proceedings of the 5th European conference on antennas and propagation (EUCAP)*, pp. 44–47.
23. Büttgen, J., et al. (2009). Mobile interaction with an NFC-based billboard. In *Adjunct Proceedings of the 11th international conference on human-computer interaction with mobile devices and services*, Bonn, Germany.
24. Cappiello, I., Puglia, S., & Vitaletti A. (2009). Design and initial evaluation of a ubiquitous touch-based remote grocery shopping process. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 9–14.
25. Chang, Y., Chang, C., Hung, Y., & Tsai, C. (2010). NCASH: NFC phone-enabled personalized context awareness smart-home environment. *Journal of Cybernetics and Systems, 41*(2), 123–145.
26. Chang, Y., et al. (2009). Toward a NFC phone-driven context awareness smart environment. In *Proceedings of symposia and workshops on ubiquitous, autonomic and trusted computing*, Brisbane, QLD, pp. 298–303.
27. Chavira, G., et al. (2007). Towards touching interaction: A simple explicit input. In *Proceedings of fourth annual international conference on mobile and ubiquitous systems: Networking & services*, Philadelphia, pp. 1–5.
28. Chen, W. D., et al. (2010). Using 3G network components to enable NFC mobile transactions and authentication. In *Proceedings of international conference on progress in informatics and computing*, pp. 441–448.
29. Chen, W. D., et al. (2011). NFC mobile payment with citizen digital certificate. In *Proceedings of 2nd international conference on next generation information technology*, Gyeongju, pp. 120–126.
30. Chen, W. (2010). NFC mobile transactions and authentication based on GSM network. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 83–89.

31. Chen, X., Lu, F., & Ye T. T. (2009). Mutual coupling of stacked UHF RFID antennas in NFC applications. In *Proceedings of IEEE antennas and propagation society international symposium*, Charleston, SC, pp. 1–4.
32. Chen, Y., et al. (2010). Analysis of antenna coupling in near-field communication systems. *IEEE Transactions on Antennas and Propagation, 58*(10), 3327–3335.
33. Cheng, H. C., et al. (2011). A secure and practical key management mechanism for NFC read–write mode. In *Proceedings on international conference on advanced communication technology*, Seoul, pp. 1095–1011.
34. Cho, J. H., et al. (2007). An NFC transceiver with RF-powered RFID transponder mode. In *Proceedings of international solid state circuits conference*, Jeju, pp. 172–175.
35. Cho, J. H., Cole, P. H., & Kim, S. (2009). An NFC transceiver using an inductive powered receiver for passive, active, RW and RFID modes. In *Proceedings of international SoC design conference (ISOCC)*, pp. 456–459.
36. Coskun, V., Ok, K., Ozdenizci, B. (2012) *Near Field Communication (NFC): From Theory to Practice*. London: Wiley. ISBN: 978-1-1199-7109-2, February, 2012.
37. Damme, G., et al. (2009). Offline NFC payments with electronic vouchers. In *Proceedings of the 1st ACM workshop on networking, systems, and applications for mobile handhelds*, pp. 25–30.
38. Dobrigkeit, P., et al. (2008). Exchange of contact data between mobile phones using NFCIP. In *Proceedings of 4th European Workshop on RFID Systems and Technologies*, Freiburg, Germany, pp. 1–9.
39. Dominikus, S., & Aigner, M. (2007). mCoupons: An application for near field communication (NFC). In *Proceedings of 21st international conference on advanced information networking and applications workshops*, Niagara Falls, pp. 421–428.
40. Dünnebeil, S., et al. (2011). Encrypted NFC emergency tags based on the German telematics infrastructure. In *Proceedings of 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 50–55.
41. ECMA International. (2004). ECMA 340: Near field communication interface and protocol (NFCIP-1). Available at: http://www.ecma-international.org/memento/TC47-M.htm.
42. ECMA International. (2006). ECMA 373: Near field communication wired interface (NFC-WI). Available at: http://www.ecma-international.org/memento/TC47-M.htm.
43. ECMA International. (2008). NFC-SEC. White paper. Available at: http://www.ecma-international.org/activities/Communications/tc47-2008-089.pdf.
44. ECMA International. (2010). ECMA 352: Near field communication interface and protocol (NFCIP-2). Available at: http://www.ecma-international.org/memento/TC47-M.htm.
45. Ervasti, M., et al. (2009). Bringing technology into school—NFC-enabled school attendance supervision. In *Proceedings of the 8th international conference on mobile and ubiquitous multimedia*. Article (4).
46. Ervasti, M., et al. (2009). Experiences from NFC supported school attendance supervision for children, In *Proceedings of third international conference on mobile ubiquitous computing, systems, services and technologies*, Sliema, pp. 22–30.
47. ETSI TS. (2008). *ETSI TS 102 613, smart cards; UICC—contactless front-end (CLF) interface; part 1: Physical and data link layer characteristics*. Technical specification.
48. ETSI TS. (2008). *ETSI TS 102 622, smart cards; UICC—contactless front-end (CLF) interface; host controller interface (HCI)*. Technical specification.
49. Finkenzeller, K. (2010). *RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. London: Wiley. ISBN: 978-0-470-69506-7.
50. Fontecha, J., et al. (2011). An NFC approach for nursing care training. In *Proceedings of 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 38–43.
51. Francis, L. (2010). A security framework model with communication protocol translator interface for enhancing NFC transactions. In *Proceedings of sixth advanced international conference on telecommunications*, Barcelona, pp. 452–461.
52. Francis, L., et al. (2010). On the security issues of NFC enabled mobile phones. In *International Journal of Internet Technology and Secured Transactions, 2*(3/4), 336–335.
53. Francis, L., et al. (2010). Practical NFC peer-to-peer relay attack using mobile phones. In *Proceedings of the 6th international conference on radio frequency identification: Security and privacy issues*, pp. 35–49.
54. Francis, L., Hancke, G., Mayes, K., & Markantonakis, K. (2009). Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms. In *Proceedings of international conference for internet technology and secured transactions*, London, pp. 1–8.

55. Franssila, H. (2010). User experiences and acceptance scenarios of NFC applications in security service field work. In *Proceedings of the second international workshop on near field communication*, Monaco, pp. 39–44.
56. Fressancourt, A., Herault, C., & Ptak, E. (2009). NFCSocial: Social networking in mobility through IMS and NFC. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 24–29.
57. Garrido, P. C., et al. (2011). Use of NFC-based pervasive games for encouraging learning and student motivation. In *Proceedings of 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 33–37.
58. Gebhart, M., & Szoncso, R. (2010). Optimizing design of smaller antennas for proximity transponders. In *Proceedings of the 2010 second international workshop on near field communication*, Monaco, pp. 77–82.
59. Ghiron, S. L., Sposato, S., Medaglia, C. M. & Moroni, A. (2009). NFC ticketing: A prototype and usability test of an NFC-based virtual ticketing application. In *Proceedings of the first international workshop on near field communication*, Hagenberg, Austria, pp. 45–50.
60. GlobalPlatform. (2009). 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.
61. GlobalPlatform. (2006). GlobalPlatform card specification, version 2.2, http://www.globalplatform.org/specificationscard.asp.
62. Globalplatform, GlobalPlatform Mobile Task Force. (2010). Requirements for NFC mobile: Management of multiple secure elements version 1.0. Available at: http://www.globalplatform.org/documents/whitepapers/GlobalPlatform_Requirements_Secure_Elements.pdf.
63. Golovashych, S. (2005). The technology of identification and authentication of financial transactions from smart cards to NFC-terminals. In *Proceedings of IEEE intelligent data acquisition and advanced computing systems: Technology and applications*, Sofia, pp. 407–412.
64. Gossar, M., et al. (2011). Investigations to achieve very high data rates for proximity coupling devices at 13.56 MHz and NFC applications. In *Proceedings of the 3rd international workshop on near field communication*, Hagenberg, Austria, pp.71–76.
65. Grunberger, S., & Langer, J. (2009). Analysis and test results of tunneling IP over NFCIP-1. In *Proceedings of the first international workshop on near field communication*, Hagenberg, Austria, pp. 93–97.
66. GSMA. (2007). Pay-buy mobile business opportunity analysis, version 1.0. White paper. Available at: http://www.gsmworld.com/documents/gsma_nfc_tech_guide_vs1.pdf.
67. Haikio, J., Tuikka, T., Siira, E., & Tormanen, V. (2010). Would you be my friend?—creating a mobile friend network with 'Hot in the City'. In *Proceedings of the 43rd Hawaii international conference on system sciences*, Hawaii, USA, pp. 1–10.
68. Hardy, R., & Rukzio, E. (2008). Touch & interact: Touch-based interaction of mobile phones with displays. In *Proceedings of the 10th international conference on human computer interaction with mobile devices and services*, pp. 245–254.
69. Hardy, R., & Rukzio, E. (2008). Touch & interact: Touch-based interaction with a tourist application. In *Proceedings of the 11th international conference on human–computer interaction with mobile devices and services*, Bonn, Germany.
70. Hardy, R., et al. (2010). MyState: Using NFC to share social and contextual information in a quick and personalized way. In *Proceedings of the 12th ACM international conference adjunct papers on ubiquitous computing*, Copenhagen, Denmark, pp. 447–448.
71. Haselsteiner, E., & Breitfuß, K. (2006). Security in near field communication (NFC)", Philips semiconductors. Available at: http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf.
72. Ho, T. & Chen, R. (2011). Leveraging NFC and LBS technologies to improve user experiences. In *Proceedings of international joint conference on service sciences*, Taiwan, pp. 17–21.
73. Hsiang, H. C., et al. (2009). A secure mCoupon scheme using near field communication. *International Journal of Innovative Computing, Information and Control, 5*(11), 3901–3909.
74. Iglesias, R., et al. (2009). Experiencing NFC-based touch for home healthcare. In *Proceedings of the 2nd international conference on pervasive technologies related to assistive environments*, Corfu, Greece.
75. Isomursu, M. (2008). Tags and the city. *PsychNology Journal, 6*(2), 131–156.
76. Ivanov, R. (2010). Indoor Navigation system for visually impaired. In *Proceedings of international conference on computer systems and technologies*, Sofia, Bulgaria.

77. Jara, A. J., et al. (2010). A pharmaceutical intelligent information system to detect allergies and adverse drugs reactions based on internet of things. In *Proceedings of 8th IEEE international conference on pervasive computing and communications workshops*, Mannheim, pp. 809–812.
78. Jara, A. J., et al. (2010). Evaluation of the security capabilities on NFC-powered devices. In *Proceedings of European workshop on smart objects: systems, technologies and applications*, Ciudad, Spain, pp. 1–9.
79. Jara, A. J., Zamora, M. A., & Skarmeta, A. F. G. (2009). Secure use of NFC in medical environments. In *Proceedings of 5th European workshop on RFID systems and technologies*, Bremen, Germany, pp. 1–8.
80. Jara, J., et al. (2010). Drugs interaction checker based on IoT. In *Proceedings of internet of things*, Tokyo, pp. 1–8.
81. Jaring, P., Tormanen, V., Siira, E., & Matinmikko, T. (2007). Improving mobile solution workflows and usability using near field communication technology. In *Proceedings of the 2007 European conference on ambient intelligence*, Darmstadt, Germany, pp. 358–373.
82. Juntunen, A., Luukkainen, S., & Tuunainen, V. K. (2010). Deploying NFC technology for mobile ticketing services-identification of critical business model issues. In *Proceedings of ninth international conference on mobile business and 2010 ninth global mobility roundtable*, pp. 82–90.
83. Kadambi, K. S., et al. (2009). Near-field communication-based secure mobile payment service. In *Proceedings of the 11th international conference on electronic commerce*, pp. 142–151.
84. Kalman, G., & Noll, J. (2007). SIM as secure key storage in communication networks. In *Proceedings of 3rd international conference on wireless and mobile communications*, Guadeloupe, pp. 55–55.
85. Karpischek, S., Michahelles, F., Bereuter, A., & Fleisch, E. (2009). A maintenance system based on near field communication. In *Proceedings of the 3rd international conference on next generation mobile applications, services and technologies*, Cardiff, Wales, UK, pp. 234–238.
86. Karpischek, S., Michahelles, F., Resatsch, F., & Fleisch, E. (2009). Mobile sales assistant—an NFC-based product information system for retailers. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 20–23.
87. Kefalakis, N., et al. (2008). Supply chain management and NFC picking demonstrations using the AspireRfid middleware platform. In *Proceedings of the ACM/IFIP/USENIX Middleware '08 conference companion*, Leuven, Belgium, pp. 66–69.
88. Kennedy, T., & Hunt, R. (2008). A review of WPAN security: Attacks and prevention. In *Proceedings of the international conference on mobile technology, applications, and systems*, Article 56.
89. Kneissl, F., et al. (2009). All-i-touch as combination of NFC and lifestyle. In *Proceedings of 1st international workshop on near field communication*, Hagenberg, Austria, pp. 51–55.
90. Köbler, F., Koene, P., Krcmar, H., Altmann, M., & Leimeister, J. M. (2010). LocaTag—an NFC-based system enhancing instant messaging tools with real-time user location. In *Proceedings of the 2nd international workshop on near field communication*, Monaco, pp. 57–61.
91. Laukkanen, M. (2007). Towards operating identity-based NFC services. In *Proceedings of IEEE international conference on pervasive services*, Istanbul, pp. 92–95.
92. Liikka, J., et al. (2008). KAMO—Mobile guide for the city traveller. In *Proceedings of 4th international conference on intelligent environments*, Seattle, WA, pp. 1–7.
93. Lin., W., et al. (2009). Optimization of NFC compatible transponder with respect to the nonlinear IC impedance. In *Proceedings of international microwave workshop on wireless sensing, local positioning*, and RFID, Croatia, pp. 1–4.
94. Lin, Y. S., et al. (2009). Near-field communication using phase-locking and pulse signaling for millimeter-scale systems. In *Proceedings of IEEE 2009 custom integrated circuits conference (CICC)*, San Jose, CA, pp. 563–566.
95. López-de-Ipiña, D. (2007). Touch computing: Simplifying human to environment interaction through NFC technology. In *1as Jornadas Científicas sobre RFID*, 21 a 23 de noviembre de 2007.
96. Lou, Z. (2010). NFC enabled smart postal system. In *Proceedings of the 2nd international workshop on near field communication*, Monaco, pp. 33–38.
97. Madlmayr, G. (2008). A mobile trusted computing architecture for a near field communication ecosystem. In *Proceedings of the 10th international conference on information integration and web-based applications & services*, pp. 563–566.
98. Madlmayr, G., et al. (2007). The benefit of using SIM application toolkit in the context of near field communication applications. In *Proceedings of international conference on the management of mobile business*, Toronto, p. 5.
99. Madlmayr, G., et al. (2008). Management of multiple cards in NFC-devices. In *Smart card research and advanced applications* (Vol. 5189/2008, pp. 149–161).

100. Madlmayr, G., et al. (2008). Managing an NFC ecosystem. In *Proceedings of 7th international conference on mobile business*, Barcelona, pp. 95–101.
101. Madlmayr, G., et al. (2008). NFC devices: Security and privacy. In *Proceedings of third international conference on availability, reliability and security*, Barcelona, pp. 642–647.
102. Madlmayr, G., Langer, J., Kantner, C., Scharinger, J., & Schaumüller-Bichl, I. (2009). Risk analysis of over-the-air transactions in an NFC ecosystem. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 87–92.
103. Mair, R. G. (2010). Protocol-independent detection of passive transponders for near-field communication systems. In *IEEE Transactions on Instrumentation and Measurement, 59*(4), 814–819.
104. Marcus, A., Davidzon, G., Law, D., Verma, N., Fletcher, R., Khan, A., et al. (2009). Using NFC-enabled mobile phones for public health in developing countries. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 30–35.
105. Michahelles, F., et al. (2007). Pervasive RFID and near field communication technology. *Journal of IEEE Computer Society, Pervasive Computing, 6*(3), 94–95.
106. Miranda, S., & Pastorelly, N. (2011). NFC mobiquitous information service prototyping at the University of Nice Sophia Antipolis and multi-mode NFC application proposal. In *Proceedings of the 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 3–8.
107. Miraz, G. M., Ruiz, I. L., & Gomez-Nieto, M. A. (2009). How NFC can be used for the compliance of European higher education area guidelines in European universities. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 3–8.
108. Miraz, G. M., Ruiz, I. L., & Gómez-Nieto, M. Á. (2009). University of things: Applications of near field communication technology in university environments. *Journal of E-Working, 3*(1), 52–64.
109. Mitrokotsa, A., et al. (2008). Classification of RFID attacks. *Journal of Information Systems Frontiers, 12*(5), 491–505.
110. Mobey Forum. (2010). 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.
111. Morak, J., Hayn, D., Kastner, P., Drobics, M., & Schreier, G. (2009). Near field communication technology as the key for data acquisition in clinical research. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 15–19.
112. Morak, J., Schwetz, V., Hayn, D., Fruhwald, F., & Schreier, G. (2008). Electronic data capture platform for clinical research based on mobile phones and near field communication technology. In *Proceedings of the 30th annual international conference of the IEEE Engineering in Medicine and Biology Society*, Vancouver, Canada, pp. 5334–5337.
113. Morris, S., & Lefley, A. (2009). A 90 nm CMOS 13.56 MHz NFC transceiver. In *Proceedings of IEEE Asian solid-state circuits conference*, Taipei, pp. 25–28.
114. Mujal, J., Ramon, E., Dí az, E., Carrabina, J., Calleja, A., Martí nez, R., & Terés, L. (2010). Inkjet printed antennas for NFC systems. In *Proceedings of 17th IEEE international conference on electronics, circuits, and systems*, pp. 1220–1223.
115. Mulliner, C. (2009). Vulnerability analysis and attacks on NFC-enabled mobile phones. In *Proceedings of international conference on availability, reliability and security*, Fukuoka, pp. 695–700.
116. Nandwani, A., et al. (2011). NFC mobile parlor games enabling direct player to player interaction. In *Proceedings of 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 21–25.
117. Neefs, J., Schrooyen, F., & Doggen, J. (2010). Paper ticketing vs. electronic ticketing based on off-line system 'Tapango'. In *Proceedings of the second international workshop on near field communication*, Monaco, pp. 3–8.
118. Nepper, P., Konrad, N., & Sandner, U. (2007). Talking media. In *Proceedings of 9th international conference on human computer interaction with mobile devices and services*, Singapore.
119. NFC Forum. (2006). *NFC data exchange format (NDEF)*. Technical specification, version 1.0.
120. NFC Forum. (2006). *Record type definition (RTD)*. Technical specification, version 1.0.
121. NFC Forum. (2006). *Smart poster record type definition*. Technical specification, version 1.1.
122. NFC Forum. (2006). *Text record type definition*. Technical specification, version 1.0.
123. NFC Forum. (2006). URI record type definition. Technical specification, version 1.0.
124. NFC Forum. (2009). *Logical link control protocol (LLCP)*. Technical specification, version 1.0.
125. NFC Forum. (2009). *NFC Forum tag types*. Available at: http://www.nfc-forum.org/resources/white_papers/NXP_BV_Type_Tags_White_Paper-Apr_09.pdf.
126. NFC Forum. (2010). *Signature record type definition*. Technical specification, version 1.0.
127. NFC Forum. Available at: http://www.nfc-forum.org.

128. Ok, K. (2010). Current benefits and future directions of NFC services. In *Proceedings of IEEE international conference on education and management technology*, Cairo, Egypt, pp. 334–338.
129. Ok, K. (2010). Exploring underlying values of NFC applications. In *Proceedings of international conference on management technology and applications*, Singapore, pp. 283–287.
130. Ok, K., Coskun, V., & Aydin, M. N. (2010). Usability of mobile voting with NFC technology. In *Proceedings of IASTED international conference on software engineering*, Innsbruck, Austria, pp. 151–158.
131. Ondrus, J., & Pigneur, Y. (2007). An assessment of NFC for future mobile payment systems. In *Proceedings of the international conference on the management of mobile business*, p. 43.
132. Opperman, C. A., et al. (2011). A generic NFC-enabled measurement system for remote monitoring and control of client-side equipment. In *Proceedings of 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 44–49.
133. Ozdenizci, B., Coskun, V., Aydin, M. & Ok, K. (2010). NFC loyal: A beneficial model to promote loyalty on smart cards of mobile devices. In *Proceedings of IEEE international conference for internet technology and secured transactions*, London, pp. 134–139.
134. Ozdenizci, B., et al. (2010). Design science in NFC research. In *Proceedings of IEEE international conference for internet technology and secured transactions*, London, pp. 158–163.
135. Ozdenizci, B., et al. (2010). NFC research framework: A literature review and future research directions. In *Proceedings of 14th international business information management association conference on global business transformation through innovation and knowledge management*, Istanbul, Turkey, pp. 2672–2685.
136. Ozdenizci, B., Ok, K., Coskun, V., & Aydin, M. (2011). Development of an indoor navigation system using NFC technology. In *Proceedings of fourth international conference on information and computing*, Phuket Island, pp. 11–14.
137. Pasquet, M., et al. (2008). Secure payment with NFC mobile phones in the smart touch project. In *Proceedings of international symposium on collaborative technologies and systems*, Irvine, CA, pp. 121–126.
138. Payez Mobile. http://www.payezmobile.com.
139. Pering, T., et al. (2007). Gesture connect: Facilitating tangible interaction with a flick of the wrist. In *Proceedings of the 1st international conference on tangible and embedded interaction*, pp. 259–262.
140. Prinz, A., et al. (2011). inSERT—an NFC-based self reporting questionnaire for patients with impaired fine motor skills. In *Proceedings of 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 26–31.
141. Resatsch, F. (2010). *Ubiquitous computing*. Wiesbaden: Gabler. ISBN: 978-3834921673.
142. Resatsch, F., et al. (2007). Mobile sales assistant—NFC for retailers. In *Proceedings of the 9th international conference on human computer interaction with mobile devices and services*, pp. 313–316.
143. Reveilhac, M., & Pasquet, M. (2009). Promising secure element alternatives for NFC technology. In *Proceedings of the first international workshop on near field communication*, Hagenberg, Austria, pp. 75–80.
144. Roland, M., & Langer, J. (2010). Digital signature records for the NFC data exchange format. In *Proceedings of 2nd international workshop on near field communication*, Monaco, pp. 71–76.
145. Roland, M., et al. (2011). Security vulnerabilities of the NDEF signature record type. In *Proceedings of the 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 65–70.
146. Roland, M., Witschnig, H., Merlin, E., & Saminger, C. (2008). Automatic impedance matching for 13.56 MHz NFC antennas. In *Proceedings of 6th international symposium on communication systems, networks and digital signal processing*, Graz, pp. 288–291.
147. Rudametkin, W., et al. (2008). NFCMuseum: An open-source middleware for augmenting museum exhibits. In *Advanced sensors and lightweight programmable middleware for innovative RFID enterprise applications*.
148. Ruiz, I., et al. (2009). University smart poster: Study of NFC technology applications for university ambient. In *Advances in soft computing*, (Vol. 51, pp. 112–116).
149. Sanchez, I., Riekki, J., & Pyykkonen, M. (2009). Touch & compose: Physical user interface for application composition in smart environments. In *Proceedings of the first international workshop on near field communication*, Hagenberg, Austria, pp. 61–66.
150. Sánchez, I., Cortés, M., & Riekki, J. (2007). Controlling multimedia players using NFC enabled mobile phones. In *Proceedings of the 6th international conference on mobile and ubiquitous multimedia*, Oulu, Finland, pp. 118–124.

151. Sánchez, I., et al. (2008). Touch & control: Interacting with services by touching RFID tags. In *Proceedings of the 2nd international workshop on RFID technology—concepts, applications, challenges (IWRT 08)*.
152. Sánchez, I., et al. (2011). NFC-based interactive learning environments for children. In *Proceedings of the 10th international conference on interaction design and children*, pp. 205–208.
153. Sandner, U., et al. (2007). News-on-the-Go. In *Proceedings of mobile HCI'07*, Singapore, pp. 361–363.
154. Schoo, P., & Paolucci, M. (2009). Do you talk to each poster? Security and privacy for interactions with web service by means of contact free tag readings. In *Proceedings of 1st international workshop on near field communication*, Hagenberg, Austria, pp. 81–86.
155. Siira, E., & Haikio, J. (2007). Experiences from near-field communication (NFC) in a meal service system. In *Proceedings of 1st annual RFID Eurasia*, Istanbul, Turkey, pp. 1–6.
156. Siira, E., & Törmänen, V. (2010). The impact of NFC on multimodal social media application. In *Proceedings of the 2nd international workshop on near field communication*, Monaco, pp. 51–56.
157. Siira, E., Tuikka, T., & Tormanen, V. (2009). Location-based mobile Wiki using NFC tag infrastructure. In *Proceedings of the 1st international workshop on near field communication*, Hagenberg, Austria, pp. 56–60.
158. Smart Trust. (2009). 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.
159. Sodor, B., Fordos, G., Doktor, T., & Benyo, B. (2011). Building a contactless university examination system using NFC. In *Proceedings of 15th IEEE international conference on intelligent engineering systems (INES)*, pp. 57–61.
160. Steffen, R., Preißinger, J., Schöllermann, T., Müller, A., & Schnabel, I. (2010). Near field communication (NFC) in an automotive environment. In *Proceedings of the 2nd international workshop on near field communication*, Monaco, pp. 15–20.
161. Strömmer, E., et al. (2006). Application of near field communication for health monitoring in daily life. In *Proceedings of 28th annual international conference of the IEEE Engineering in Medicine and Biology Society*, New York City, USA, pp. 3246–3249.
162. Tuikka, T., & Isomursu, M. (2009). *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.
163. Verdult, R., & Kooman, F. (2011). Practical attacks on NFC enabled cell phones. In *Proceedings of the 3rd international workshop on near field communication*, Hagenberg, Austria, pp. 77–82.
164. Vergara, M., Díaz-Hellín, P., Fontecha, J., Hervás, R., Sánchez-Barba, C., Fuentes, C., et al. (2010). Mobile prescription: An NFC-based proposal for AAL. In *Proceedings of the 2nd international workshop on near field communication*, Monaco, pp. 27–32.
165. Wiechert, T., et al. (2009). NFC based service innovation in retail: An explorative study. In *Proceedings of ECIS'2009*.
166. Wiethoff, A., & Broll, G. (2011). SoloFind: Chains of interactions with a mobile retail experience system. In *Proceedings of the 2011 annual conference extended abstracts on human factors in computing systems*, Vancouver, BC, pp. 1303–1308.
167. Woo, J. (2008). Verification of receipts from M-commerce transactions on NFC cellular phones. In *Proceedings of 10th IEEE conference on E-commerce technology and the fifth IEEE conference on enterprise computing, E-commerce and E-services*, Washington, DC, pp. 36–43.
168. Yiqun, X., et al. (2008). Sales data management system of chain enterprises based on NFC technology. In *Proceedings of 2nd international conference on anti-counterfeiting, security and identification*, Guiyang, pp. 455–458.
169. Zhao, M., et al. (2010). A chip solution for UWB-NFC receiver in CMOS 0.18um technology. In *Proceedings of the 6th international wireless communications and mobile computing conference*, pp. 839–842.

Author Biographies

Vedat Coskun is a Computer Scientist, Academician, and Author. He established NFCLab – Istanbul (www.NFCLab.com), the leading and pioneer research lab on Near Field Communication (NFC) technology worldwide, which aims to take initiative on sustainable evolution of the technology for creating a win-win ecosystem for all the actors in the game such as users and financial and technical organizations. He is currently working as Associate Professor of Information Technology department in ISIK University, Istanbul. He received "Excellence in Teaching" award from ISIK University in 2012. He also gave lectures in several other universities such as University of Thessaly/Volos, Greece, Malardalen University/Vasteras, Sweden, Inholland University/Amsterdam, Netherlands. He is specialized in Security, Mobile Technologies, Java technology, Android, and NFC. He has vast amount of conference and journal publications. He authored several books, including Near Field Communication: From Theory to Practice, which is published in 2012 by John Wiley & Sons Inc. He believes on the importance of academia & industry relationship, and takes role as consultant for national and international companies in this manner.

Busra Ozdenizci received her MS degree in Information Technologies from ISIK University, Turkey and currently studying her Ph.D. degree in Computer Engineering in Yeditepe University, Turkey. Her research areas include Near Field Communication, Mobile Communication Technologies and Mobile Persuasion. She is a member of NFC Lab – Istanbul. She also co-authored Near Field Communication: From Theory to Practice, which is published in 2012 by John Wiley & Sons Inc. She is a member of NFC Lab – Istanbul.

Kerem Ok received his M.S. degree from ISIK University, Turkey and currently studying his Ph.D. degree in Information Technology in Istanbul University, Turkey. His research areas include RFID, Near Field Communication, Mobile Communication Technologies and Object Oriented Technology. He is a member of NFC Lab - Istanbul. He also co-authored Near Field Communication: From Theory to Practice, which is published in 2012 by John Wiley & Sons Inc.