1

Executive Summary

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

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

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

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

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

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

phone manufacturers have already put their NFC enabled mobile phones into the market. As NFC enabled mobile phones spread and commercial services are launched, people will be able to pay for goods and services, access hotel rooms or apartments, update their information in social networks, upload their health data to hospital monitoring systems from their homes, and benefit from many more services by using their NFC enabled phones.

The success of NFC technology is bound to advances in other fields as well. Over-the-Air (OTA) technology among ecosystem actors is definitely a prerequisite to operate NFC systems satisfactorily. Secure Element (SE) is also a requirement to store valuable digital information and to provide concurrent execution of multiple NFC services on the same smart card securely. Dependence on other technologies is one of the challenges that NFC currently faces now.

Another important challenge is about the potential stakeholders in the NFC ecosystem. NFC has a complex and dynamic environment with high number of participating organizations. They have already recognized the possible added values, and each party is trying to maximize the value of their stake. The ownership and management of the SE is a dominant factor in getting a greater share, because each transaction has to use some applications installed on the SE, and the owner can always demand a higher share. Currently Mobile Network Operators (MNOs) own and issue the UICC as SE on mobile phones, and alternative SE ownerships are being negotiated among MNOs financial organizations, and even smart card manufacturers.

Please note that this chapter is an executive summary of the book and hence references are provided at the end of the related chapters.

1.1 Towards NFC Era

NFC is a technology that simplifies and secures the interaction with the automation ubiquitously around us. The NFC concept is designed from the synergy of several technologies including wireless communications, mobile devices, mobile applications and smart cards. Server side programming, web services, and XML technologies also contribute fast improvement and the spread of NFC technology. Many daily applications, such as credit cards, car keys, and hotel room access cards will presumably cease to exist because an NFC enabled mobile phone will suffice to provide all of their functionalities.

Currently, NFC is one of the enablers for ubiquitous computing. Therefore the origin of the idea is closely related to ubiquitous computing. In order to understand the relation of NFC and ubiquitous computing, we need to start with the history of ubiquitous computing.

1.1.1 Ubiquitous Computing

The essence of modern computers is automated calculation and programmability. The history of modern computers includes the work of pioneers over almost two hundred years. Personal Computers (PCs) are an important step after early computers, changing the way that a user interacts with computers by using keyboards and monitors for input and output instead of punch cards, cables and so on. The mouse has also changed the way humans and computers interact because it enabled users to input spatial data to a computer. The hand became accustomed to holding the mouse, and the pointing finger became accustomed to clicking it. The movements of the pointing device are echoed on the screen by the movements of the cursor, creating a simple and intuitive way to navigate a computer's Graphical User Interface (GUI).

Touch screens changed the form of interaction dramatically. They removed the need for earlier input devices, and the interaction was performed by directly touching the screen, the new input device. In the meantime, mobile phones had been introduced, initially for voice communication. Early forms of mobiles contained a keypad. Mobile phones with touch screens can be assumed to be the state of the art technology as the same screen is used as both the input and output unit, allowing the user to act more intuitively.

Ubiquitous computing is the highest level of interaction between humans and computers, where computing devices are completely integrated into everyday life and the objects around, and are simple to use. Ubiquitous computing is a model in which humans do not design their activities according to the machines they need to use; instead, the machines adjust to human needs. Eventually, the primary aim is that humans using machines will not need to change their normal behaviors and also will not even notice that they are performing activities with the help of machines.

1.1.2 Mobile Phones

A mobile phone is an electronic device which is primarily used to make voice calls while the user is mobile. The user of the mobile phone must be registered to a mobile phone network where the service is provided by a MNO. The call can be made to or received from any other phone which is a member of either the same or another mobile phone network, a fixed line network, or even an internet based network. Mobile phones support the anytime, anywhere motto. Mobile phones are also referred to as mobiles.

Mobile phones are very convenient to use and handy. Therefore in addition to the voice call capability, a vast amount of additional services are bundled to it, and many new future services are still on the way, such as NFC technology. Currently supported mobile phone communication services can be viewed based on whether they are wired or wireless services. Mobile phones also include a vast amount of integrated services.

USB and PC synchronization are the most significant wired services. The phones are connected to the computers to enable data transfer, synchronization and so on.

The amount of wireless services, on the other hand, is much greater. GSM communication is obviously the primary service that a mobile phone provides. As a matter of fact it was the one that the pioneer phones provided. Later, Short Messaging Service (SMS) was introduced. Multimedia Messaging Service (MMS) could be enabled only after high data transfer rates between the base stations and the mobile phones. Moreover, users can experience mobile radio and television services with mobile phones. Localization services, specifically Global Positioning System (GPS), allowed phones to enable applications such as navigation and social media interaction. One added communication capability to mobile phones is via several peer-to-peer services such as Infrared, Bluetooth, and finally NFC. Infrared requires line of sight, NFC requires very close interaction, namely touching, and Bluetooth requires communication within small distance. Wi-Fi connectivity allowed mobile phones to access the Internet with low bandwidth. Electronic mail (e-mail) enabled users to access their inboxes or send e-mails while mobile.

Storing contact and communication details are the most important integrated services, since they simplify Global System for Mobile Communications (GSM). There are other integrated services that are not related to GSM, at least not directly. Instead, the main objective of those

services is to eliminate additional devices and integrate all into one device. Calculator is one primitive function and eliminates the physical need for a calculator. Gaming is the one that most people like to have in their mobiles. Taking photos and videos, and even editing them using additional applications are simple to use so that additional cameras or video recorders are not required. Music and video playback are two other attractive facilities. Moreover, clock and alarm capability has removed the need for watches.

Some major wireless services currently enabled by mobile phones are GPS Navigation, Wireless Internet services, GSM, Bluetooth, Wi-Fi, and NFC technologies.

1.1.3 Technological Motivation of NFC

The main motivation for NFC is the integration of personal and private information such as credit card or debit card data into mobile phones. Therefore, security is the most important concern, and the wireless communication range provided even by RFID technology is considered too long. Mechanisms such as shielding are necessary to prevent unauthorized people from eavesdropping on private information because even non-powered, passive tags can be read over 10 m. This is where NFC comes in.

1.1.4 Wireless Communication, RFID, and NFC

Wireless communication refers to data transfer without using any cables. When communication is impossible and impractical for cable usage, wireless communication is the solution. The communication range may vary from a few centimeters to many kilometers. Wireless is generally mobile, and mobile is essentially wireless. We also distinguish nomadic communication from mobile. Devices that allow nomadic communication may perform either wireless or wired communication at a given time. An example of nomadic communication is the laptop.

The direct consequence of wireless communication is mobility. Mobility allowed people to be flexible, since they can be reached anywhere. It is obvious that mobility increased productivity, since mobile communication enabled people to be reached at anytime and anywhere. This has a big impact on our daily lives. People become reachable not only for commercial purposes, but also for social reasons. The currently available mobile communication services that support mobility are GSM, Bluetooth, Wi-Fi, WiMAX, and ZigBee.

1.2 Evolution of NFC

NFC can be taught as an extension to RFID that also uses smart card technologies' interfaces. To understand NFC technology, we need to have a brief knowledge of the forerunners of NFC technology: the barcode as an earlier form of RFID technology, RFID, and the magnetic stripe card as an earlier form of smart cards and smart card technologies.

1.2.1 Earlier Form of RFID: Barcode Technology

A barcode is a visual representation of data of the object to which it is attached. The information on the barcodes is scanned by barcode readers and transferred to the computing devices that are connected to the readers. Then the device processes the information.

Early barcodes represent data by varying the widths and spacing of parallel lines, and are referred to as linear or one-dimensional (1D). Due to the used space, minimum thickness of each bar and orientation restrictions, the maximum addressable 1D code is not high. In contrary to limited number of available 1D codes, later two-dimensional (2D) barcodes evolved which have a larger data storage capacity. As an example, 2D barcodes on a medicine box may contain specific identification information for that medicine box, so each specific patient and each specific medicine can be tracked.

Some major examples of linear barcodes are UPC (Universal Product Code) and EAN13 (European Article Number) Barcodes. Also QR (Quick Response) Code Barcode is an example of a 2D barcode.

1.2.2 RFID Technology

RFID is a technology that uses communication via radio waves to exchange data between an RFID reader and an electronic RFID tag (label), traditionally attached to an object, mostly for the purpose of identification and tracking. The data transmission results from electromagnetic waves, which can have different ranges depending on the frequency and the magnetic field.

RFID tags are small integrated circuits which can hold small applications as well as tiny amount of data. There are two types of RFID tags; passive tags and active tags. Passive tags have no internal power supply, have an IC (Integrated Circuit) and antenna embedded in them. They are powered by the incoming signal from a Radio Frequency (RF) field. Passive tags have practical read distances ranging from about 10 cm up to a few meters depending on the chosen RF and antenna design and size. Unlike passive RFID tags, active RFID tags have their own internal power source which is used to power any ICs that generate the outgoing signal. Active tags are typically much more reliable than passive tags due to the ability to conduct a session with a reader at longer distances. The major drawback of RFID tags when compared with paper barcodes is their higher price.

Both barcodes and RFID tags can be copied, however in different ways. Barcodes can be distributed electronically which enables printing and displaying on a digital device such as a PC or a mobile phone. You can e-mail a barcode image to a vast number of people and all of the receivers can print the barcode onto ordinary paper immediately. RFID tag content can be electronically spread as well. However, a digital chip is required for each copy instead of paper. When compared with barcodes, producing the original as well as copies is more expensive. The RFID tag has large data capacity, and each individual tag has a unique code which is similar to 2D barcodes. The uniqueness of RFID tags provides a product that can be tracked as it moves from one location to another.

RFID was a relatively early technology, and many RFID applications have been developed so far. Some of those applications are as follows:

- *Inventory control:* Most RFID applications are for managing assets. Retail stores use RFID tags on their items to control purchase, decrease in inventory and so on.
- *Toll roads:* Active RFID tags are fixed on vehicles so that during the vehicle's journey, the toll cost can easily be deducted from the owner's account.

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

1.2.3 Earlier Form of Smart Cards: Magnetic Stripe Cards

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

1.2.4 Smart Card Technology

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

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

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

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

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

The popular cards are the proximity contactless smart cards which enable a wide range of usage in a wide range of areas from health to entertainment. Various proximity coupling smart card technologies have emerged; however, only a few of them have become ISO/IEC 14443 standard which also provides interface for NFC transactions depending on the operating modes. Currently, the most famous and competing proximity contactless smart cards are MIFARE, Calypso, and FeliCa.

(i) *MIFARE*
MIFARE is a well-known and widely used 13.56 MHz contactless proximity smart card system that is being developed and is owned by NXP Semiconductors which is a spin-off company of Philips Semiconductors. MIFARE is ISO/IEC 14443 Type A Standard. Today, MIFARE is used in more than 80% of all contactless smart cards in the world.

(ii) *Calypso*
Calypso is an international electronic ticketing standard for a microprocessor contactless smartcard, originally designed by a group of European transit operators from Belgium, Germany, France, Italy and Portugal. It ensures multi-sources of compatible products, and makes possible the interoperability between several transport operators in the same area.

(iii) *FeliCa*
FeliCa is a 13.56 MHz contactless proximity high speed smart card system from Sony and is primarily used in electronic money cards. However, FeliCa did not become an ISO/IEC standard.

1.2.5 NFC as a New Technology

NFC operates between two devices over a very short communication range. NFC communication uses the 13.56 MHz spectrum as in RFID. Currently data transfer speed options are 106, 212, and 424 kbps. NFC technology operates in different operating modes; reader/writer, peer-to-peer, and card emulation where communication occurs between an NFC mobile on one side, and a passive RFID tag (NFC tag), an NFC mobile or an NFC reader on the other side. NFC technology is compared with the other technologies in terms of data transfer rate in Chapter 2, Figure 2.23. One of the NFC technology's major properties is its implicit security because of short communication distance. Close proximity of two devices makes the signal interception probability very low. The other property is the automatic implicit pairing capability of NFC. An installed application on a mobile device is automatically launched when it finds the matching pair.

1.3 NFC Essentials

As the basics of the used technology are provided above, we can now introduce essential NFC technical details. In order to do this, NFC structure and the NFC devices (NFC tag, NFC reader, and NFC mobile) must be explained in enough detail. The communication is based on the existing standards, and the devices stick to those standards for a seamless activation. Hence, we also will provide information on the standardization bodies which steer NFC technology.

1.3.1 Smart NFC Devices

NFC devices are the acting components of NFC. NFC is available using three NFC devices: the NFC mobile, NFC reader and NFC tag.

- *NFC enabled mobile phone:* NFC enabled mobile phones which are also referred to as NFC mobiles are the most important NFC devices. Currently, integration of NFC technology with mobile phones (thus introducing NFC enabled mobile phones) creates a big opportunity for the ease of use and acceptance of the NFC ecosystem.
- *NFC reader:* An NFC reader is capable of data transfer with an NFC component. The most common example is the contactless POS (Point of Sale) terminal which can perform contactless NFC enabled payments when an NFC device is touched against the NFC reader.
- *NFC tag:* An NFC tag is actually an RFID tag that has no integrated power source.

NFC works in a very intuitive way. Two NFC devices immediately start their communication as they are touched. The touching action is taken as the triggering condition for NFC communication. This is actually an important feature of NFC technology. In the NFC case, the NFC application is designed so that when the mobile touches some NFC component with the expected form of data, it boots up. Hence, the user does not need to interact with the mobile device after she touches one appropriate NFC device which may be an NFC tag, an NFC reader, or another NFC enabled mobile phone. This is a very useful property of NFC communication that provides ubiquitous computing.

For each NFC communication session, the party that starts or initiates the communication is called the initiator, whereas the device that responds to the requests of the initiator is called the target. This case is analogous to the well-known client server architecture. Remember that in a client server communication the client initiates the communication and the server responds. In NFC communication, it is no different.

In an active/passive device approach, when an NFC component has an embedded power source, it can generate its own RF field, and naturally initiates and leads communication. This device is called an active device. On the other hand, if it does not have any embedded power source, it is called a passive device and can only respond to the active device.

The initiator always needs to be an active device, because it requires a power source to initiate the communication. The target, however, may be either an active or a passive device. If the target is an active device, then it uses its own power source to respond; if it is a passive device, it uses the energy created by the electromagnetic field which is generated by the initiator that is an active device.

Consider an NFC tag which is a low cost and low capacity device. It does not contain any power source and needs an external power source to perform any activity. Thus, an NFC tag is always a passive device and always a target, since it does not include any energy source by design. It stores data that can be read by an active device.

1.3.2 Standardization of NFC Enabled Mobile Phones

NFC technology was jointly developed by Philips and Sony in late 2002 for contactless communications. Europe's ECMA International adopted the technology as a standard in December

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

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

(i) *NFC Forum*

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

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

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

(ii) *GlobalPlatform*

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

(iii) *GSM Association* (*GSMA*)

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

(iv) *ISO/IEC*

ISO is the world's largest developer and publisher of international standards. It is a non-governmental organization that forms a bridge between the public and private sectors. IEC is a non-profit international organization that prepares and publishes international standards for all electrical, electronic and related technologies. ISO and IEC work together to provide worldwide standards.

(v) *ECMA International*

ECMA International is an international non-profit standardization organization for information and communications systems. ECMA studies include mobile devices and NFC.

(vi) *ETSI and ETSI Smart Card Platform* (*ETSI SCP*)

ETSI is a non-profit organization with 700+ members. The ETSI produces globally applicable standards for Information and Communications Technologies (ICT), including fixed/mobile, radio, broadcast and Internet technologies. ETSI SCP handles Subscriber Identity Module (SIM) specifications that would enable SIM cards to carry NFC applications or to play other roles within NFC phones.

(vii) *Java Community Process* (*JCP*)

JCP holds the responsibility for the development of Java technology which indeed is a prominent candidate for NFC applications as well. As an open, inclusive organization of active members and non-member public input, it primarily guides the development and approval of Java technical specifications.

(viii) *Open Mobile Alliance* (*OMA*)

OMA develops open standards for the mobile phone industry. OMA members include many companies including the world's leading mobile operators, device and network suppliers, information technology companies and content and service providers.

(ix) *3rd Generation Partnership Project* (*3GPP*)

3GPP is a collaboration between groups of telecommunications associations to make a globally applicable third generation (3G) mobile phone system specification. 3GPP specifications are based on evolved GSM specifications.

(x) *EMVCo*

EMVCo aims to ensure global interoperability between chip cards and terminals on a global basis regardless of the manufacturer, the financial institution or the card issuer. EMV 2000 specifications are an open standard set for smart card based payment systems worldwide and seek collaboration in mobile payment standards.

1.3.3 General Architecture of NFC Enabled Mobile Phones

Mobile devices those are integrated with NFC technology contain NFC specific ICs such as SEs and an NFC interface (see Chapter 3, Figure 3.7). The NFC interface is composed of an analog/digital front-end called an NFC Contactless Front-end (NFC CLF), an NFC antenna and an NFC controller to enable NFC communication. The NFC controller enables NFC communication of the mobile phone with the external NFC device. An NFC enabled mobile phone requires an SE for performing secure transactions with the external NFC devices. The SE provides a secure environment for related programs and data. It enables storage of sensitive data of the user. It also enables secure storage and execution of NFC enabled services such as

contactless payments. Various standards have already been defined for NFC communication between two NFC enabled devices, and data transfer within the NFC mobile phone such as Single Wire Protocol (SWP) or the NFC Wired Interface (NFC-WI).

The host controller can be identified as the heart of any mobile phone. A Host Controller Interface (HCI) creates a bridge between the NFC controller and the host controller. The HCI is a logical interface which allows an NFC interface including front-end to communicate directly with an application processor and multiple SEs in mobile devices.

1.3.4 Near Field Communication Interface and Protocol (NFCIP)

At the physical layer, the Near Field Communication Interface and Protocol (NFCIP) is standardized in two forms as NFCIP-1 which defines the NFC communication modes on the RF layer and other technical features of the RF layer, and NFCIP-2 which supports mode switching by detecting and selecting one communication mode.

(i) *Near Field Communication Interface and Protocol-1 (NFCIP-1)*
NFCIP-1 standard defines two communication modes as active and passive. It also defines RF field, RF communication signal interface, and general protocol flow. Moreover, it defines transport protocol including protocol activation, data exchange protocol with frame architecture and error detecting code calculation (CRC for both communication mode at each data rate), and protocol deactivation methods.

(ii) *Near Field Communication Interface and Protocol-2 (NFCIP-2)*
NFCIP-2 standard specifies the communication mode selection mechanism and is designed not to disturb any on-going communication at 13.56 MHz for devices implementing NFCIP-1, ISO/IEC 14443 and ISO/IEC 15693.

1.4 NFC Operating Modes and Essentials

Remember that there may three major smart devices in NFC; NFC enabled mobile phones, NFC readers, and NFC tags. NFC communication occurs between two NFC devices with some valid combinations. For example, a mobile phone may communicate with an NFC reader.

As NFC occurs within a very close range, it is very common to touch the communicating devices against each other. For this reason, this process is called touching paradigm. User awareness is definitely a must in order to perform NFC. The user first interacts with a smart object (that is either an NFC tag, NFC reader, or another NFC mobile) using a mobile phone (see Chapter 4, Figure 4.3). After the touching activity occurs, the mobile device may make use of the received data and use mobile services as well, such as opening a web page, making a web service connection and so on.

1.4.1 NFC Operating Modes

There are three operating modes, reader/writer, peer-to-peer, and card emulation, as already mentioned. The reader/writer mode enables one NFC mobile to exchange data with one NFC tag. The peer-to-peer mode enables two NFC enabled mobiles to exchange data with each

other. In card emulation mode, a mobile phone can be used as a smart card to interact with an NFC reader. Each operating mode has a different technical infrastructure as well as benefits for the users.

(i) *Reader/writer mode*
This mode provides communication of an NFC mobile with an NFC tag. The purpose of the communication is either reading or writing data from or to a tag by the mobile phone. We can further categorize the mode into two different modes: reader mode and writer mode. In reader mode, the mobile reads data from an NFC tag; whereas in writer mode, the mobile phone writes data to an NFC tag.

(ii) *Peer-to-peer mode*
Two NFC mobiles using this mode exchange any data between each other. Since both mobiles have integrated power, each one uses its own energy by being in active mode in this mode. Bidirectional half duplex communication is performed in this mode similar to other modes, meaning that when one device is transmitting, the other has to listen and can start transmitting data after the first one finishes.

(iii) *Card emulation mode*
This mode provides the opportunity for an NFC mobile to function as a contactless smart card. Some examples of emulated contactless smart card are credit cards, debit cards, loyalty cards and so on. One NFC mobile may even store multiple contactless smart card applications concurrently. The card emulation mode is an important mode since it enables payment and ticketing applications and is compatible with existing smart card infrastructure.

1.4.2 Reader/Writer Mode Essentials

As already mentioned, the underlying technical architecture of each mode differs. The standards and specifications used by each mode may also differ. In reader/writer operating mode, an active NFC enabled mobile phone initiates the wireless communication, and can read and alter data stored in NFC tags. First, the used RF interface in this mode is compliant to ISO/IEC 14443 Type A, Type B and FeliCa schemes which are contactless smart card interfaces (see Chapter 3, Figure 3.24). The applications operating in reader/writer mode usually do not need a secure area in the NFC enabled mobile phone; the process is only reading data stored inside the tag and writing data to the tag.

In this operating mode, NFC Forum performed various specifications and standards in tag types, operation of tag types, and data exchange format between devices. An NFC enabled mobile phone is capable of reading NFC Forum mandated tag types. Four tag types have been defined by NFC Forum, and are designated as Type 1, Type 2, Type 3 and Type 4. Each tag type has a different format and capacity. NFC tag type formats are based on either ISO 14443 Type A, ISO 14443 Type B, or Sony FeliCa.

The other important standard is the NDEF. NDEF is a data format to exchange information between two NFC devices; namely, between an active NFC mobile and a passive tag, or an active NFC mobile and an active NFC mobile.

NDEF is a binary message format designed to encapsulate one or more application-defined payloads into a single message construct. An NDEF message contains one or more NDEF

records and those records can be chained together to support larger payloads. Various record types for NDEF messaging format are defined by NFC Forum for specific cases; smart posters, URIs, digital signature, and text.

The record types defined for smart posters are the most used. For example, with the defined smart poster record types, URLs, SMSs or phone numbers can be put on an NFC Forum mandated tag. By touching an NFC device to the tag, this information can be read and processed afterwards. The smart poster contains data that will trigger an application in the device such as launching a browser to view a website, sending an SMS to a premium service to receive a ring tone, and so on.

1.4.3 Peer-to-Peer Mode Essentials

In peer-to-peer mode, two NFC enabled mobile phones establish a bidirectional, link level connection to exchange information as depicted in Chapter 3, Figure 3.29. They can exchange virtual business cards, digital photos, and any other kind of data or perform Bluetooth pairing, and so on. Peer-to-peer operating mode's RF communication interface is standardized by ISO/IEC 18092 as NFCIP-1. Also NDEF message is used in this mode which is received over LLCP that is also defined by NFC Forum. The data format is the same as that used in reader/writer mode.

LLCP as a data link layer protocol supports peer-to-peer communication between two NFC enabled devices which is essential for any NFC application that involves a bidirectional communication. LLCP specification defines five major services: connectionless transport, connection oriented transport, link activation-supervision-deactivation, asynchronous balanced communication and protocol multiplexing.

1.4.4 Card Emulation Mode Essentials

In card emulation mode, an NFC enabled mobile phone acts as a smart card. Either an NFC enabled mobile phone emulates an ISO 14443 smart card or a smart card chip integrated in a mobile phone is connected to the antenna of the NFC module. When the user touches the mobile phone to an NFC reader, the NFC reader initiates the communication. This operating mode is useful for secure transactions such as contactless payment, ticketing applications and access control.

As depicted in Chapter 3, Figure 3.32, when an NFC reader interacts with an NFC device, the NFC device acts like a standard smart card, thus the NFC reader interacts with the SE and its applications. Only the card emulation mode uses an SE efficiently and performs functions securely.

1.4.5 Case Studies

We present the following three case studies at the end of Chapter 4 to clarify the three operating modes and their usages thoroughly:

1. The NFC enabled shopping system enables users to shop online anywhere they want, so that no geographical restrictions are set. This use case employs the reader/writer mode.

2. The NFC based gossiping application works in the same way as gossiping and disseminates information between the parties. This use case employs the peer-to-peer mode.
3. The cinema ticketing application enables payment to be made. This use case employs the card emulation mode.

In each use case, initially the description of the case is given. Use case diagrams, activity diagrams, and generic usage models follow. The first and second use cases are also implemented with Java in Chapter 5. The codes may run in emulator or mobile phone after successful implementation. The third use case's ecosystem environment and business models are analyzed in Chapter 7.

1.5 SE and Its Management

In order to provide secure storage and execution of NFC enabled applications, an SE is essential. The SE is actually a combination of hardware, software, interfaces, and protocols. Since secure functions are mostly provided in card emulation mode, an SE is mostly used in that mode as well. When an SE is used appropriately, that is, according to the provided standards, the users and service providers are assured about the security of the overall process. Currently various SE alternatives are being considered, but the most popular ones are (see Chapter 3, Figure 3.10):

- Embedded hardware;
- Secure Memory Card (SMC);
- Universal Integrated Circuit Card (UICC).

(i) *Embedded hardware*

The embedded SE is a non-removable component within a mobile phone. This chip is embedded into a mobile phone during the manufacturing stage and it must be personalized after the device is delivered to the end user. This embedded SE chip obviously cannot be transferred to other mobile phones. It has to be replaced and personalized every time the mobile phone is used by another user. The SE of a new mobile phone must be personalized for the user.

(ii) *SMC*

A removable SMC is made up of memory, embedded smart card element and smart card controller. In other words, it is a combination of a memory card and a smart card. With the removable property and a large capacity memory, the SMC based SE can host a large number of applications, and does not need to be reissued when the customer buys a new mobile phone.

(iii) *UICC*

The UICC is the physical smart card that the Subscriber Identity Module (SIM) or Universal Subscriber Identity Module (USIM) is implemented upon. Therefore it is commonly known as a SIM or USIM. A UICC based SE is a removable smart card used in mobile terminals in GSM and UMTS networks.

A UICC based SE provides an ideal environment for NFC applications. It is personal, secure, portable and easily managed remotely via OTA technology. The card holder can be assured that transactions are executed with their personal information protected. It has appropriate card structure based on the GlobalPlatform card specification that allows multiple security domains for different applications on the same smart card. By use of OTA, new NFC applications can remotely be installed onto the UICC easily, personalized afterwards, and the life cycle of the SE can be managed easily thereafter. Hence, the user does not need to physically touch the NFC enabled mobile device to a system in order to perform any of the processes mentioned.

1.5.1 Over-the-Air Technology

OTA is the standard for exchanging applications and application related information through wireless communications media. By facilitating an OTA platform, new services can be introduced; the SEs can be accessed, manipulated, and modified in a rapid and cost effective way through an OTA platform. Based on the ecosystem that has been agreed upon, the OTA service can be provided by an MNO or another trusted entity.

Currently, UICC cards are produced, submitted to the user, and hence owned by the MNOs in an ad hoc fashion. MNOs control and manage the UICC, and use OTA functionality provided by the same MNO to manage the UICC. Hence, OTA capabilities are considered as part of the main functionalities of MNOs as well as part of mobile device management.

1.5.2 GlobalPlatform Card Specification

Remember that GlobalPlatform card specification contains the details of the smart card. Based on the standards defined by the GlobalPlatform, the logical and physical components of the smart card aim to provide application interoperability and security in an issuer controlled environment.

Security domains are extremely important for the GlobalPlatform based smart cards to provide enough level of security. As a matter of fact, security domains are the on-card representatives of off-card authorities. They enable management of applications in a secure fashion by providing a complete separation of cryptographic keys and the security domains can be categorized, reflecting different types of off-card authority recognized by a card:

- The Issuer Security Domain (ISD) is the on-card representative of the card issuer. This component represents the issuer's area on the card that controls the issuer's applications.
- The Supplementary Security Domain (SSD) is the on-card representative of the application providers and card issuers. This component allows the application providers to share and utilize a territory on the card without the risk of compromising management of the card or any application on the card.
- The Controlling Authority Security Domain (CASD) is actually a sub type of SSD. The role of the controlling authority is to enforce security policy to all applications on the card.

1.5.3 Trusted Service Manager

In order to deploy NFC applications and services onto the user's SEs, service providers and MNOs have distinct requirements. To create and manage a trusted environment and to allow actors to communicate among themselves securely, an additional trusted actor is required; Trusted Service Manager (TSM) which is an independent party serving the other actors of the NFC ecosystem as required. The TSM ensures a level of trust and confidentiality between major actors of the system such as service providers and MNOs during the application life-cycle management.

1.5.4 UICC Management Models

GlobalPlatform smart card standards define the card content management process to contain several activities: loading the initial key set of the security domain, application coding of a third party, application loading, personalization and so on.

GlobalPlatform defines three card content management models as simple mode, delegated mode and authorized mode. These models cover application loading and personalization processes on SEs. The simple mode is a completely card issuer centric model, whereas the delegated mode and authorized mode are more TSM centric models. GlobalPlatform messaging specification supports all deployment models.

(i) *Simple mode using MNO OTA platform*
In simple mode, the service provider delegates full management of its NFC enabled application to a TSM. TSM manages the security domain on behalf of the service provider. MNO is authorized to perform the card content management functions, namely loading, installing, activating and removing the application on the SE. TSM only manages the application lock, unlock, and personalization processes using its own OTA server and network of the MNO.

(ii) *Delegated mode with full delegation to the TSM*
The delegated management case can be described as TSM centric loading. In this case the MNO is no longer in charge of loading, installing, activating or removing the application. Card content management is performed by the TSM with a pre-authorization from the MNO. In some cases, the service provider may need to manage its own application personalization process to prevent any third party manipulation of application keys or application data.

(iii) *Authorized mode with full delegation to TSM*
The authorized management deployment is completely organized around the TSM centric loading option. TSM has service provider applications, and is able to perform card content management without authorization (or being forced to use a token) from the MNO. As in delegated mode, the service provider can manage its own application personalization instead of delegating it to the TSM.

1.5.5 Multiple SE Environments

It is also possible to see that a single NFC enabled mobile phone can host multiple SEs. For example, a mobile phone may contain an embedded hardware or SMC that is integrated

by the manufacturer during the production process, together with an UICC based SE that is embedded by the MNO before handing the mobile phone to the customer. Many problems may emerge when multiple SEs reside on the same NFC enabled mobile handset. One of the problems can emerge when implementing card emulation mode applications. The NFC reader needs to initiate communication with only one SE on the NFC enabled mobile phone. Another problem is the management of multiple SEs at the same time. According to GlobalPlatform, two business models can be performed: architecture without aggregation and architecture with aggregation:

- *Architecture without aggregation*: The NFC controller can be used by only one SE at a given time, thus only one SE can be active at a time. The SE is activated by the user so that the activated SE is able to perform NFC enabled contactless transactions. The user is responsible for selecting the correct SE in this model.
- *Architecture with aggregation*: All SEs hosted in NFC enabled mobile phones are active at the same time. Any application on any SE can perform contactless NFC transactions at any given time. Obviously each SE can contain one or more applications. The application should be selectable by the external NFC reader.

1.6 NFC Application Development

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. The first one is a Graphical User Interface (GUI) application which exists in all operating mode applications. A GUI application provides an interface which allows a user to interact with the mobile device. It also provides the capability to read and write from and to NFC components. The second type is an SE application which is needed in order to provide a secure and trusted environment for security required applications (e.g., credit card). 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 Symbian^3 mobile phones;
- Series 40 Nokia 6212 NFC SDK for Nokia 6212 devices.

Java is a well-known object-oriented programming language, and can be used in various environments from PCs to refrigerators, and from servers to mobile phones. Java, in the NFC context, provided one of the first APIs (Application Programming Interfaces). We have provided information on how to develop NFC applications using Java in Chapter 5. Lessons learned from Chapter 5 will help users develop NFC based applications in other development platforms as well.

Java provides two APIs for NFC development: JSR 257 (Contactless Communication API) and JSR 177 (Security and Trust Services API). JSR 257 mainly enables reader/writer mode application programming resources, whereas JSR 177 and some classes in JSR 257 provide access to SEs to implement card emulation mode projects. For peer-to-peer mode

Table 1.1 JSR 257 packages

Package	Description
javax.microedition.contactless	Provides common functionalities to all contactless targets such as discovering the target
javax.microedition.contactless.ndef	Provides functionality to exchange NFC Forum formatted data with RFID tags
javax.microedition.contactless.rf	Enables communication with RFID tags that contain non-NFC Forum formatted data
javax.microedition.contactless.sc	Enables communication with ISO14443-4 smart cards
javax.microedition.contactless.visual	Enables communication with visual tags

programming, propriety APIs are required, since this mode is not supported by the standard Java APIs.

1.6.1 JSR 257

This API provides an application programming interface that allows applications to access RFID tags, smart cards, and visual tags (bar codes). Different packages are defined for each target type and an application using this API can discover contactless targets in the proximity, notify applications upon discovery and perform contactless operations. A few classes in this API also allow access to SEs using ISO 14443 connection. Table 1.1 summarizes the packages in JSR 257.

1.6.2 JSR 177

This API defines optional packages to support smart card communication and security operations. Digital signature services, user credential management, cryptographic operations and more can be implemented using this API. It enables mobile phones to access smart cards using APDU (Application Protocol Data Unit) and JavaCard Remote Method Invocation (RMI) protocols. JSR 177 consists of four optional packages (summarized in Table 1.2) which also consist of different packages and classes.

Table 1.2 JSR 177 packages

Optional Package	Description
SATSA-APDU	Enables communication with smart cards using a protocol based on APDUs
SATSA-JCRMI	Enables communication with smart cards using JavaCard RMI protocol
SATSA-PKI	Enables smart cards to manage digital signatures and certificates
SATSA-CRYPTO	Provides cryptographic operations such as message digests and digital signatures to increase security

Peer-to-peer mode is not supported by standard Java APIs; however, there are extensions to Contactless Communication API that provide programming in peer-to-peer mode. These are generally mobile device specific APIs, namely proprietary APIs.

Push registry is another important topic in NFC and can increase the usability of applications. Normally, applications can be executed by a user's action from the mobile phone's menu. However, an application can also run without any user action, but with the 'Push' feature. For example, an application can be triggered with a network package received by an incoming SMS. Push registry simply maintains a list of inbound connections and runs applications automatically based on received connections. In the case of NFC, it enables applications to launch with an NFC connection.

In order to activate a push registry service, an application should be registered to run with a specified connection. Two types of registrations are possible: dynamic and static. With static registration, an application is registered for a push record when installing it in the mobile device. On the other hand, dynamic registration is performed at the first execution of the application.

Dynamic and static registrations have their own advantages and disadvantages. Static registration enables a push connection to register easily without a user's action at installation stage. However, if there is a conflicting push registry entry in the device, the application cannot be installed. On the other hand, dynamic registration eliminates this issue. One disadvantage of dynamic registration is that in order to save the push registry record, the first execution of the application needs to be performed with a user's action.

1.7 NFC Security and Privacy

Although a mobile phone is almost identical to a PC in technical terms, it is different since it is more a personal item and mostly carried by people in daily life. Users generally believe that their mobile phones are an important part of their lives and they usually put them under physical surveillance. However, a mobile phone is still subject to physical attacks such as theft, and technical wireless attacks using Bluetooth or WI-FI communication technologies. Integrated NFC capability also imposes some additional risks to mobile phones.

1.7.1 Why is Security Important?

A service is useful only when it is both functional and secure enough. A user initially cares about the functionality, and only subsequently notices the importance of the security. In conclusion, a user is eager to use a service only when it is functional and yet secure. Technical deficiencies and security related obstacles are potentially of concern to users.

People were not aware of the importance of the security of services decades ago. As malicious activities started to emerge, both people and companies started to notice the importance of security but only after the cost of the damage became sizeable. The hackers also noticed that they could gain financially in addition to being proud of gaining illegal access to the assets and causing damage as well.

There are some obvious reasons why the security risk has increased so much lately. Three viewpoints are given.

Hackers' point of view:

- They may get financial reward.
- They may satisfy their egos.
- They may even become famous when they perform incredibly successful actions.

Users' point of view:

- The number of Internet users is increasing exponentially; hence the opportunity for malicious actions is also increasing. One hacker can try the same method to hack many potential victims.
- The amount of financial assets has grown, resulting in greater financial reward to hack.

Technical point of view:

- Organizations traditionally ignore security during the initial stage of software development. One reason for this is to keep expenditure within the budget, and security seems the most obvious area in which to reduce costs. This results in failure in security of the system even if a vast amount of effort is spent subsequently, since it is not easy to integrate security if it is ignored during the design phase.

Now it is time to make a projection of the importance of security in general in the NFC ecosystem. The major reasons why NFC is an alluring target are:

- NFC is an emerging technology and integrated with mobile phones.
- Nearly everybody owns a mobile.
- NFC is heavily promoted by service providers, MNOs, and banks.
- NFC potentially has a big financial market, which is tempting for the hackers.

1.7.2 Primary Goals of Security Measures

The security requirements of each system are different; their priorities are different as well. Some prioritize keeping the information available to only one or more people, while others demand keeping the application data contents unchanged by illegal parties.

The most common security requirements can be listed as follows:

- Secrecy ensures that information is accessible only to those with authorized access.
- Authentication approves the identity of a person, a process, or a device based on the provided information.
- Authorization allows different actions on the object (file, application, or machine) by the subject (user) after authentication is provided.
- Non-repudiation of a party prevents the sender from denying sending a message to the receiver, so that a referee can prove the case.
- Availability ensures that the system responds correctly and completely to the requests of the authorized users at any given time.

- Data integrity ensures that the received information is exactly the same as the information sent, and thus confirms that it has not been accidentally or maliciously modified, altered, or destroyed.
- Accountability guarantees tracing back all the actions together with the actor who performs.

1.7.3 Vulnerability, Threat, Attack, and Risk

In order for a malicious action to create damage on the secured system, initially the system should be vulnerable to attacks. In this sense, vulnerability is a weakness in a system which allows an attacker to perform some actions that threatens its information assurance.

A threat is a possible danger that may cause an unfair benefit to the unauthorized user or cause harm by making use of vulnerability.

An intentional attempt by intruders to perform an unauthorized access to information is called an attack.

Attacks are classified as active or passive. If an attack does not modify or delete a resource it is classified as passive, otherwise it is classified as an active attack.

The potential harm that may arise after the realization of some threat is further defined as the risk.

1.7.4 Security Tools and Mechanisms

In order to satisfy the security requirements, cryptography is the primarily used technique. Most of the security mechanisms rely on cryptography. Cryptography is used for providing a secure channel, storing password information within the hard disk, digitally signing the financial transactions, and so on.

Cryptography is also used for many purposes such as hiding the content of the data from an unauthorized third party, or preventing illegal modification of some transmitted data. The following are the basic services that are provided by cryptography:

- The stored or exchanged information is not revealed to the unauthorized parties.
- The content of the stored or exchanged data cannot be changed by unauthorized parties, or it will be noticed if it occurs.
- When the data are created or sent by some party, the party cannot deny creating or sending them.

In cryptography the original data (plaintext) is initially encrypted by using an encryption key to create a modified form of the plaintext, called the ciphertext. The data can simply be stored or be transferred to the receiver. The receiver decrypts the data by using the decryption key in order to recreate the original message.

The idea of satisfying secrecy using cryptography is being able to send the message in a scrambled form called a ciphertext, so that communication between the sender and the receiver is still possible, and can be performed using public channels such as the Internet.

1.7.5 NFC Security

As with all information systems, NFC based systems are subject to attacks that threaten system security and user privacy. Each operating mode of NFC has a different architecture. Hence, attacks and defense mechanisms are mostly subject to different use cases. When NFC based systems are analyzed from the security point of view, we should consider the security concerns related to the NFC tag, NFC reader, smart card, communication and backend systems separately.

1.7.5.1 Security Issues on NFC Tag

Remember that the NFC tag is involved in reader/writer mode. In this mode traditionally an NFC mobile interacts with an NFC tag. In order to satisfy the overall security requirements, the security of the data on the NFC tag as well as the security of the communication between NFC devices must be secured. Remembering that the NFC tag is actually an RFID tag, we can make use of the knowledge that is accumulated by using RFID tags to handle the security of the same tag in NFC. Traditionally, the following are the security issues related to the NFC, or RFID tag:

(i) *Tag cloning*
The attacker may try to clone, or create an exact copy of a valid tag. In order to insert preventive mechanisms to the system, applications that require high processing capability are required, increasing the cost of low-cost tags. Obviously this is unfeasible and unacceptable, since the major point here is enabling low-cost NFC tags.

(ii) *Tag content changes*
The attacker may try to modify an NFC tag to change its content. In this way, several attacks become possible:
- Spoofing attacks
  Spoofing attack is providing false information to the user which seems valid, and hence possibly will be accepted by the user. By spoofing attack, the user may insert a fake domain name, telephone number or false information about the identification of some person, item, or activity on to the tag.
- Manipulating tag data
  The content of the tag might be changed by the attacker for some malicious purpose.
- Denial of Service (DOS) attack.
  DoS attacks aim to damage the relationship between the customer and the service provider. The primary way to do this is by exhausting the system's resources by forcing it to perform some unnecessary and illegal action. This results in decreasing and eventually exhausting the power source of the server.

(iii) *Tag replacement and tag hiding*
The NFC tag may be replaced by a malicious tag, so that the latter tag performs illegal actions as it is designed to do. Sticking a malicious tag on top of the original tag or replacing the original tag with a malicious tag is called tag hiding, and is enough to let the system work as the attacker desires.

1.7.5.2 Security Issues on NFC Reader

Remember that card emulation mode involves the interaction of the mobile phone with the NFC reader. Hence, security of the reader is the concern in this mode. An NFC reader is similar to the RFID reader; therefore the security concerns are consequently similar. These kinds of similarities are important and reassuring, since the potential problems have been mostly solved up to now.

1.7.5.3 Security Issues on Smart Cards

Smart cards on the mobile phone are mostly used by applications operating in card emulation mode in an NFC ecosystem. Hence, the security of a smart card is a major concern in this mode. The attacks on smart cards can be categorized into two groups: invasive attacks and side channel attacks.

1.7.5.4 Security Issues on Communication

In all operating modes of NFC technology, it is obvious that a short range communication is used. Attackers with enhanced radio devices can communicate with the contactless smart cards within several meters. Therefore, attacks and threats during the communication are valid in all modes.

- *Eavesdropping:* An unauthorized individual may use an antenna in order to record communication between NFC devices.
- *Data Corruption:* In addition to eavesdropping, an attacker can try to modify the transmitted data.
- *Data Modification:* The attacker may try to modify or delete valuable information by intercepting the communication.
- *Data Insertion:* Data may be inserted into the exchanged messages between two NFC devices. The attacker must be fast enough to send the data before the valid responder. The insertion will be successful only if the inserted data can be transmitted before the original device responds. If both data streams overlap, the data will be corrupted.
- *Man-in-the-Middle Attack:* These attacks are performed by unknown parties in a communication, who relay information back and forth by giving the simultaneous appearance of being the other party.
- *Relay Attack:* The attacker uses wireless communication to borrow the data from the victim's tag into another tag. This means that the attacker inserts messages into the exchanged data between two devices.
- *Replay Attack:* A valid NFC signal is intercepted and its data is recorded first; this is later transmitted to a reader so that it is "played back". Since the data appear valid, the reader accepts them unless suitable prevention mechanisms are used.

1.7.5.5 Middleware and Backend System Security

An NFC based system contains NFC readers, NFC mobiles and NFC tags in technical terms. A complete NFC system includes servers to store and manage data such as banking servers, credit

card middleware, authentication subsystems, and so on. Hence, security of an NFC system is not complete unless the security of all components of the system is provided. Security issues of the middleware and the backend systems are not within the scope of this book. However, the reader should be aware of the fact that the middleware and backend systems should be secure.

1.7.5.6 Standardized NFC Security Protocols

All NFC related security protocols are standardized in ECMA 385 as NFC-SEC and in ECMA 386 as NFC-SEC-01. These protocols deal with the NFCIP-1 security issues since NFCIP-1 provides no security at all. NFC-SEC provides security standard for peer-to-peer NFC communication. On top of NFCIP-1, NFC-SEC is promoted to insert security capabilities.

1.7.6 Privacy, Legal, and Ethical Aspects

Information that is voluntarily shared but is later stolen or misused is an important issue nowadays. Privacy requires the appropriate use of information. When something is private to a person, it usually means that it is considered inherently and personally special. Privacy is broader than security and includes the concepts of appropriate use and protection of information.

A few decades ago it was considered to be the information era. Now is regarded to be the age of information management. The reason for this difference is obvious: data and information are everywhere. It is more important to retrieve the useful information than to create it.

A huge amount of data is generated by various means all over the world. Data are collected worldwide using sensors, applications, and other data collecting devices. Wireless sensor nodes and cameras are two examples of data collecting devices. When you call somebody or even carry your mobile without using it intentionally, buy something even by using cash, or click on a website on your browser, many data are recorded. Hence, generating data is no longer a problem. The issue is how to make use of the data.

It is true that people do not like to be recorded when entering a building, walking on a road, meeting a friend in a café, and so on. It is unfortunate that this trend will not be changed even if it can be slowed down temporarily. It is even more annoying if the captured data are used in activities invading users' privacy.

The rules must be changed worldwide, because currently it is so easy to use the information gathered about people even without their permission.

1.7.6.1 What to do to Protect Privacy

It is true that wireless communication is subject to a higher number of security risks when compared with wired media. It is also true that mobile devices have lower processing capability because of higher hardware cost, which results in vulnerability in carrying out services implemented to build security measures.

Another fact is that companies traditionally cared about the security of the products much less than the functionality. Hence, initially people were happy when they bought new applications,

but then encountered damage as the vulnerabilities were misused by malicious actions. Hence, public suspicion towards the new technology greatly increased.

Since the public became more suspicious of mobile and wireless systems, RFID also received public opposition as well. Hence, RFID met with fear and rejection over time.

In the RFID case, customers complained when they were not informed by companies that they had embedded RFID tags to their products. Even if they had been informed, the customers were not told of all the risks. Hence, people became angry when they eventually learned the facts. It is possible to leak sensitive data that is on the tag especially if the individual is unaware of the tag.

Since NFC is an emerging technology, the collection, storage and usage of sensitive private data is of public concern as well. Valuable private data such as payment card information and personal identity information are at risk when appropriate measures are not taken.

In order to appease public concern, detailed information as well as all the risks should be given to the potential customers and appropriate security measures should be applied as well. In order to achieve the trust of users there is a clear need for effective tools that support users to protect their privacy. Supporting data protection legislations, other legal measurements and auditing mechanisms can also be required. In this way, NFC application users might be convinced that these applications will not misuse their personal data and privacy.

1.8 NFC Business Ecosystem

Many technological improvements have been introduced so far. Some historical examples include radio receivers, televisions, cable television channels, satellite television channels, phones, mobile phones and satellite phones. Some of these technologies have been successfully accepted whilst others have just disappeared. There are various reasons for acceptance or rejection of such technologies. The primary requirement for wide usage of such technology is technical success of course. Without technical sufficiency, no technical device can be used.

The next factor that affects the success of the technology is public acceptance. If people find it useful enough, then they are eager to pay for it. As more people pay for the devices, the companies earn more income and provide further investment to improve the technology. As the technology is improved the unit price is reduced, which makes more people willing to own the device. This cycle carries the price of the item to a reasonable level so that the new technology eventually becomes successful.

As we can see from the last paragraph, the dominant factor of the success of the model is actually more financial than technological. Economical motivations enable technical sufficiency over a period of time. We have already examined the user's involvement in the process. From the investor's perspective, the Return of Investment (RoI) is the primary motivation of companies. Companies always request a small timeframe in which to get their money back.

It is true that in any technological device usage, there is more than one company involved. Consider television broadcasting for example. There are manufacturers, cable companies, advertisement firms, infrastructure firms and many others. Each company tries to maximize their profit, thus decreasing their RoI as much as possible. We can illustrate the financial aspect using a cake. The size of the cake is affected by the number of users that are willing to pay money for the products and services. The share of each company is then defined. Each company tries to get the most. If the resultant sharing set-up is healthy then the system

works. In contrast, if any major company cannot receive enough money, its RoI increases too much and hence that company does not invest any money. Let us use the television case again. If the television manufacturer tries to get most of the money by increasing the cost of the televisions, people will stop buying televisions, and hence nobody wins. As another alternative, if the channel service provider requests too much money, then people will stop purchasing televisions, since they will not be willing to use televisions any more. Hence, a good agreement on who gets what and how defines the success of the outcome.

NFC technology is no different. A success story will be written only when the players agree on how to share the profit, which is not settled yet.

It is true that the NFC ecosystem exposes an inviting financial share to all related partners. NFC creates a new business environment and large value chain. The financial shares whet the appetite of many companies.

The potential of NFC technology in business opportunities (especially in the mobile financial services industry) has caused great excitement in many organizations. Since NFC technology is made up of several components, it cuts across boundaries of many organizations from diverse business sectors.

The leading companies that might be enthusiastic about the emerging ecosystem are MNOs, banking and payment services, product manufacturers including mobile handset makers, software developers, and other merchants including transport operators and retailers.

Some worldwide companies try to get all possible profit from the NFC ecosystem. Some MNOs for example, try to circumvent the banks in order to get all the added value. The same is true for some banks as well. Some mobile manufacturers try to create appropriate models so that they will not need any MNOs or banks for facilitating NFC services. This is rather disappointing though. What the companies should understand is that no single company can get all the profit. The money to be shared can be increased only when all related sectors agree upon a share model which satisfies all companies. Otherwise, the money to be shared will only be a small amount.

NFC take-off has been slower than expected. The reason for this is not technical. The foremost reason is the lack of formation of a common understanding and vision in NFC technology among participating organizations and industries. Thus a mutually beneficial business model could not be sustained yet. The main reasons for this lack of common understanding and vision are:

- The profit that will be shared is enormous. Hence every company is eager to get a big share.
- All parties are powerful companies so that they assume that the other parties are obliged to follow their demands.
- Different technical solutions and infrastructures for a specific NFC enabled service are an issue as each party proposes a model which brings more advantage to itself than others. For example, MNOs propose SIM based models, since they can control the SIM cards and hence can receive more profit if this model is used. Nobody tries to find solutions that would possibly make all parties happy.

To achieve a fair and yet a profitable business model, interoperability, compatibility and standardization of an NFC technology model that is agreed upon are essential. It is also important to get customer acceptance.

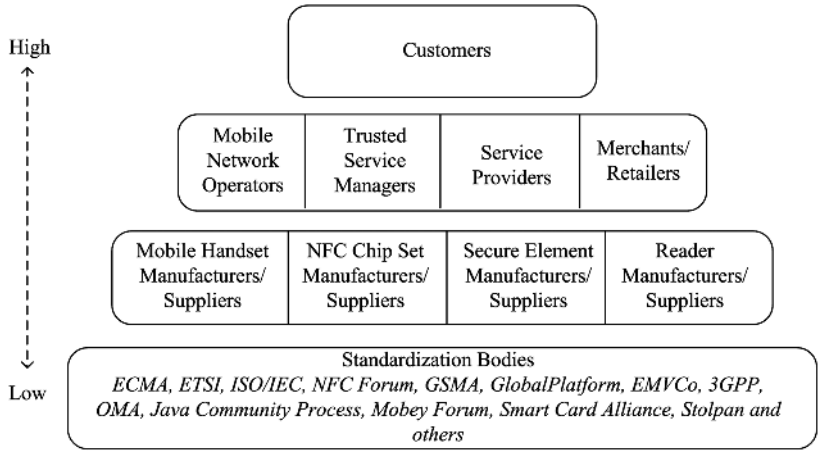

Figure 1.1 Stakeholders in NFC ecosystem.

1.8.1 Stakeholders in NFC Ecosystem

A wide range of stakeholders are potentially involved in each NFC project depending on the type of services provided. Some of the potentially leading services are smart poster, payment, ticketing, and social media processing. The type of the used service defines the potential players, details of the need for collaboration among those players, the money to be shared and so on.

As depicted in Figure 1.1, we can examine the participating entities within the NFC ecosystem on four levels. At the lowest level the standardization bodies exist who aim to develop global, interoperable standards for NFC and its dependent technologies such as smart cards and mobile phones. This level can be seen as the fundamental level for NFC technology and its ecosystem. The next level involves the hardware (i.e., mobile handset, NFC chip set, SE, NFC reader) manufacturers and suppliers. They are responsible for producing and selling products conforming to standards for enabling NFC based systems. For instance consider SE manufacturers and suppliers. They need to provide appropriate SEs to the right customers. Embedded hardware and secure memory card based SEs need to be manufactured for the mobile handset manufacturers or other retailers, and UICC based SE for MNOs. UICC manufacturers and suppliers are contracted and forced to provide required UICC hardware to the MNOs. Thus, they have a direct relationship with the MNO, who also defines the requirements for the UICCs and issues the SE.

The major players exist in the next level. These parties are the ones who effectuate the NFC enabled applications and services in a secure, trusted environment. They can be described as follows:

- MNOs traditionally provide mobile phone owners access to the communication and data network. They are actually currently responsible for – indeed have the privilege of – providing all kinds of mobile services to their subscribers. MNOs, in the meantime, can provide and maintain the network infrastructure that enables the secure OTA solutions to provide remote management and maintenance of applications stored on SEs.

- TSM is required to create and manage a trusted environment among actors of the NFC ecosystem. TSM generally offers a single point of contact with MNOs for service providers such as financial institutions, banks, transit authorities, retailers and others who want to provide a payment, ticketing, or loyalty application to customers with NFC enabled mobile phones.
- The service provider deploys as well as manages a service to the mobile devices of its customers. A service provider may be a financial institution, bank, transport authority, or some other organization.
- In the NFC ecosystem context, merchants and retailers are the stakeholders who are accepting contactless proximity mobile payment services.

These actors have a direct relationship with the end users as customers at the highest level. Customers are always the principal stakeholders in any business and are the focus of service providers; the reason for this is obvious. Customers will sustain the business only if their needs are met. All marketing activities always focus on them.

As already mentioned, several NFC trials have been implemented around the world since 2005; and operators, banks, and SE issuers are ambitious to increase their revenue through NFC services. Especially in European industry, banks and MNOs are competing industries, thus different business models and approaches can be seen to enable NFC services. For example, in Austria some MNOs have obtained banking licenses, so that they are able to provide financial and banking services. The Mobile Virtual Network Operator (MVNO) model has gained popularity in recent years. MVNOs allow MNOs and non-telecom companies to participate in mobile services. For example, in the Netherlands, a bank called Rabobank started to act as an MVNO by collaborating with an MNO to provide mobile services with financial services to its customers. Such an MVNO model creates a win–win model through MNO cooperation; the model has been rapidly expanding in countries such as Spain, Italy, and Portugal and more recently Turkey. MVNOs can increase their brand awareness, distribution channels, and customer base to provide value added services to their customers. On the other hand, MNOs can increase their network capacity, IT infrastructure and service portfolio, add a new revenue stream and so on.

1.8.2 Understanding NFC Business Models

In NFC business models, problems to be solved are mostly business related issues than technology or infrastructure related. Business models are important to deliver value to all stakeholders. Some business models do not encourage strong cooperation between all bodies; however in NFC it is a must.

Currently, there is a pervasive amount of uncertainty on which business model is the best; which firm will perform exactly which activity, and who will pay whom for which service and eventually how much profit is to be earned or shared by any stakeholder. Due to the novelty of the NFC technology, there is still no agreement or common vision of a business model that sufficiently satisfies all stakeholders. Actually, many business model proposals and specifications have been published and various projects are implemented through a vast number of trials throughout the world, especially in mobile financial services due to the high degree of complexity in ecosystem and technological infrastructure. NFC Forum, GlobalPlatform,

GSMA, and EMVCo are some of the important associations who intensively work on the NFC ecosystem and business models as well as work on the underlying technological infrastructure.

In summary, it is essential to harmonize the interests of all participants in forming sustainable business models. Otherwise conflicting, not feasible, and not interoperable solutions will be performed, and hence the technology will not be able to be improved.

There are some key questions that help us to understand the business environment of NFC enabled applications and services. These questions are:

- Who will issue and own the control of the SE?
- Who will manage the life cycle of the SE platform?
- Whose OTA platform will be used for management of the SE platform?

Relating to these questions, we have identified three main issues that determine business model alternatives for NFC; SE issuer, platform manager, and OTA provider. These issues can also be referred to as functional roles and responsibilities that need to be handled by a single entity or multiple entities in an NFC business model.

(i) *SE Issuer*

The SE issuer is the entity who issues and owns the SE. Currently, in almost all cases MNOs or service providers (e.g., banks) concurrently play the role of the SE issuer. In an ideal case, the SE issuer should be an independent actor, but currently this is not the case.

If UICC based SE is used in a business model, MNO holds the responsibility of SE issuer, since the SE is given to the user when the SIM containing the SE is provided. If embedded hardware based SE is used, the actor who gives the mobile phone to the user plays the role. If the mobile phone is given to the current customer of a MNO within the context of a campaign for example, the MNO is the card issuer. If the mobile is purchased by the user from a retailer or from a service provider, the card issuer can be any independent partner theoretically such as the retailer, service provider or other.

(ii) *Platform Manager*

The second important issue is the control and management of the SE platform. The platform manager owns the cryptographic keys that are used to control the SE in its lifecycle. The platform manager allows authorized service providers to install applications on the SE preferably using an OTA infrastructure.

The business model is simpler when the SE issuer and platform manager are the same entity. Delegating the platform manager role to some other party than the SE issuer is yet another option. Indeed this entity can be a TSM as an independent neutral party. In order to realize this option, the TSM and SE issuer previously agree on the business model. The agreement possibly consists of the details from technical infrastructure to revenue sharing. The TSM can handle all SE management functions by using its own OTA platform or MNO OTA link, which is the third important issue covered next.

(iii) *OTA Provider*

The final important issue is about the provision of the OTA Platform. Providing a flexible and interoperable OTA solution is a key requirement in the NFC ecosystem. It enables secure wireless communication between two end parties and provides transmission and reception of application related information in a wireless communication system. OTA

enables remote download, installation, and management of applications such as updating, activating or deactivating an application stored on SE.

1.8.3 Business Model Approaches

Currently available business models are MNO centric, distributed, and TSM centric alternatives:

(i) *MNO centric business model*
In the MNO centric business model, MNO issues SEs, and acts as SE issuer, platform manager and OTA provider at the same time. There is no other independent trusted entity; MNO performs all capabilities of TSM, owns, and manages the life cycle of SE using its own OTA platform. MNO also performs loading, installation, and personalization processes, as well as security domain creation on the SE. Service providers have to pay the MNO in order for their applications to run on the SE, and even share their personalization data with the MNO.

(ii) *Distributed business model*
In the distributed business model, the platform management services are distributed between the SE issuer and the service provider. There can be a separate TSM infrastructure, and using no infrastructure is still another option as well. Actually the choice depends on the entity's TSM capabilities. If the service provider has no TSM capabilities, they need to make an agreement with an existing TSM. Currently service providers prefer to collaborate with trusted third parties rather than making high investments to build OTA infrastructure within their organizations.

(iii) *TSM centric business model*
For an NFC service, a single TSM centric business model is actually the best option and a less complex business model at the same time. MNOs and service providers that want to participate in that specific NFC service ecosystem need to sign and agree with an existing TSM in the market. The TSM performs the platform manager's role completely on behalf of the service providers; this is done by realizing loading, installation, and personalization processes via its own OTA platform. The number of TSMs may increase depending on the available services and the agreements of the actors in the NFC ecosystem. For instance, NFC enabled payment and transportation services may use the same TSM platform as well as different TSM platforms.

In order to create a sustainable model, it is really important to create a win–win business model for all stakeholders in a market with many additional revenue and marketing opportunities. In order to move forward successfully with all kinds of business models, understanding the business requirements of all stakeholders especially MNOs and service providers, and establishing trust between them is essential. A secure and simple ecosystem can be acquired afterwards.

1.9 Usability in NFC

NFC technology is declared as easy to use and simple in NFC Forum. In order to use NFC, all a user needs to perform is to hold NFC enabled devices together. In this way, users can

access services, set up connections, make payment, or use a ticket [1]. Up to now, only a few studies have performed usability analysis on NFC to measure the success of trials. Here we summarize some of the studies on NFC usability.

In [2] subjective usability of a student council voting is studied and compared with a 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 [3] also performed usability tests on NFC to identify how NFC based systems could be used to improve mobile solution workflows 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 following problems:

- Access to real-time information, applications and instructions in the field;
- Real time updating of data;
- Removal of human errors;
- Reducing users' memory payload;
- Creating ability to verify people's presence in different locations.

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.

Another study on user experiences and acceptance scenarios of NFC applications [4] showed that simple NFC technology must beat the alternative technologies in terms of user experience and performance criteria especially when both technologies provide nearly the same end-user functionalities.

1.10 Benefits of NFC Applications

Numerous NFC applications are designed, prototyped, and developed so far. Service providers are eager to offer NFC based services, however sometimes they do not decide which service to offer. A study [5] analyzed most of the NFC applications in the literature and highlighted the benefits of those applications from the users' perspective. In addition, the study gave possible future usage scenarios based on the discovered benefits.

The study initially identified that each operating mode provides different benefits to users [5]. Thus they analyzed applications based on the used operating mode.

In reader/writer mode, data stored in an NFC tag are read by an NFC enabled mobile phone and then it is used to process further operations. Transferred data can be any type of text, such as a web address, data of an event, or some other data. After transfer operation, the data can be used for many purposes (e.g., display information on a mobile device's screen on the go). Moreover, based on the design of the application, this mode is able to provide mobility and to

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

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

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

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

1.10.1 Future Scenarios on NFC

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

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

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

coupling of mobile phones with the human body actually fits with the usage of mobile phones. In the near future, there may be the opportunity for people to carry NFC enabled mobile phones not only to gain mobility, but also to perform daily functions. Credit cards, keys, and tickets will be embedded into mobile phones. Hence, there will be more opportunities to integrate daily objects into NFC enabled mobile phones. In addition to the current usage areas, many objects such as identification cards, passports, fingerprints, and driver licenses can be stored in mobile phones and be employed by making use of NFC. As the mobile phone becomes part of human daily life, additional opportunities may also arise. One opportunity will be using NFC enabled mobile phones as a memory area for users' data. One of the most concrete examples of this usage is to store the user's patient information into an NFC enabled mobile phone.

1.11 NFC Throughout the World

There have been many attempts to realize NFC technology so far. Some models are developed by universities, others by companies, and even more by a joint effort between universities and companies. Many models are only theoretical, some cannot be used because of missing features but others are completely developed.

NFC city describes an area where several NFC applications are being used. The purpose of an NFC city may be either to test an implementation, or even to actually use one. NFC cities are important for the improvement of NFC technology, since they are the actual arena of a moderate sized usage media.

In NFC trials and projects, applications and the NFC ecosystem are tested; thus usability issues together with the problems of the technology can be obtained through the tests in the initial phase of NFC cities. NFC technology, applications and usability issues can be tested during this phase. During the testing period, one of the purposes is to evaluate the applicability of the NFC technology. However, it is not the only reason for this effort. One major aim is to test NFC ecosystem issues. The NFC ecosystem usability is at least as important as the technical appropriateness, since the model cannot be used when there is disagreement between the actors involved.

1.11.1 NFC Cities

1.11.1.1 City of Oulu

Oulu City was used as a test bed for the SmartTouch project. The project ran from 2006 to the end of 2008 and examined the role of NFC in city life, the home, wellbeing and health, entertainment, technological, and business building blocks. Citizens living in Oulu had the opportunity to test commercial and public NFC services as the first users of the technology over a broad aspect. The main applications that were tested are:

- Meal ordering for the elderly;
- Attendance process of students in a secondary school;
- Attendance process for a primary school using NFC;
- City orienteering for schools;
- Smart parking by eliminating coins and parking tickets;

- Retrieving news, and downloading videos from smart posters at theaters;
- Ordering lunch quickly at restaurants and obtaining coupons;
- Bus ticketing;
- Work time management and drivers' diary;
- Lock management in public sport halls;
- Information tags in the city environment;
- Future shop concept;
- NFC enabled blood glucose meter.

1.11.1.2 City of Nice

Nice is assumed to be the first NFC city in Europe with a commercial NFC roll out by every French MNO. The projects are conducted mainly on travel, m-tourism, healthcare, assisted living, m-payment, m-culture, m-government, m-education and fair trade. Implemented projects in Nice consist of all operating modes; reader/writer, peer-to-peer and card emulation modes. Also applications are stored and implemented on a single SIM card. The projects are developed in France, Morocco, Russia and Haiti with different partnerships and contracts.

These projects also involved the University of Nice hosting an important NFC pilot project in 2010–2011. The Nice Future Campus project's aim is to replace the physical student ID card with NFC enabled mobile phones and to enable multiple applications on a single SIM card. A student using this project was able to pay, manage tickets and coupons, share an opinion regarding a book, get contextual information, communicate with her friends and much more with her NFC enabled mobile phone within the campus. The main applications provided by NFC technology were for payment, the university restaurant ticket, library access, access control, location based services, social networking, and information services.

1.11.1.3 Smart Urban Spaces

Smart Urban Spaces (SUS) is a collaborative European project focusing on designing and adopting context aware services and e-city services based on NFC with the latest mobile and ubiquitous technologies. SUS is a three year project running from mid 2009 to mid 2012 and involves four countries: Finland, France, Spain and Greece. Oulu, Helsinki, Caen, Valencia and Seville are some of the cities included. The SUS project involves many organizations from all of the four countries. The main purposes of the SUS project are to provide a framework for adopting e-city services, technical and operational service analysis, interoperability analysis and testing other issues through pilots and trials. The e-city services included in the SUS projects can be categorized as transport, family and community, leisure, culture and sports, utility tools, education and learning, NFC city ecosystem, and other specific services.

1.11.2 NFC Trials and Projects

There have been various NFC trials and projects all over the world. Payment and ticketing applications are possibly the most well-known and promising everyday applications of NFC technology, and are the most complex from the ecosystem aspect as well. Thus, most of the tests

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

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

1.12 Status of Academic Research on NFC Literature

Today, NFC has become an attractive research area for many academicians due to its exploding growth and its promising applications and related services. Due to its nature, a large proportion of NFC research can be represented as design science research which aims to propose an innovative design artifact and has problem relevance and a rigorous nature. A study on NFC [6] provides a rigorous academic review on NFC literature. For the last few years, there has been a considerable increase in the number of research papers and activities concerning NFC. However, a better understanding of the current status of the NFC research area through an academic review of literature is necessary to maintain the advancement of knowledge in NFC research and to identify the gap between theory and practice.

The conducted survey is based on articles in journals and mostly conference proceeding papers. The study exclude master theses, doctoral dissertations, textbooks, unpublished working papers, white papers, editorials, news reports, and book reviews. Researchers and practitioners often use journal papers to acquire information and to disseminate new research findings, thus most of the existing literature reviews exclude conference proceeding papers too. However, conference papers are not excluded which provide "the high level of research, both in width and breadth" after journals.

(i) *NFC research framework*

In accordance with the study, an NFC research framework is proposed which includes a content-oriented classification of the NFC literature. This framework classifies the NFC academic literature in four major categories and signifies the bidirectional relationships between categories: NFC Theory and Development, NFC Infrastructure, NFC Applications and Services, and NFC Ecosystem (see Figure 1.2). Most of the papers in NFC research can be considered as design science research which provides an innovative, purposeful design artifact in the form of a construct, a model, a method, or an instantiation. The design artifact has to solve a specific problem or develop technology based solutions.

The NFC Theory and Development level is the fundamental level of the NFC research framework. It includes the studies related to the development of NFC technology and applications; "Overviews, Context and Foundations" includes general introductions, assessments, reviews about NFC, foundations and standards on NFC technology, performance analysis and measurements and new guidelines for the development of NFC enabled applications or services, and "Policy, Legal and Ethical Issues" includes security and privacy issues, regulations, and legal requirements. The papers in this category focus on more behavioral issues and behavioral sciences which seek to develop and justify theories, rather than developing a design artifact. Papers dealing with this level influence upper levels that focus on design science in NFC research.

The NFC Infrastructure level is the intermediate level that includes studies related to "Network and Communication" issues (e.g., data aspect, new communication protocols, and OTA transactions), hardware issues dealing with "Tags, Antenna, Reader and NFC Chip", "Security and Privacy" issues (e.g., vulnerability analysis, availability, confidentiality, integrity, authentication, authorization, and non-repudiation) that focus on developing design artifacts rather than behavioral issues. This layer is positioned with pre-defined business related to existing technology infrastructure, applications, and the existing ecosystem. The proposed framework shows the direct linkages of NFC

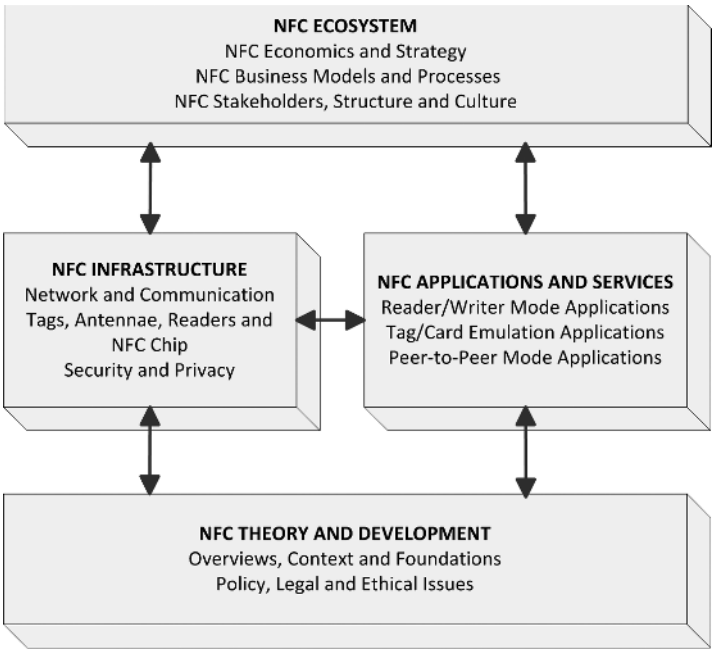

Figure 1.2 Classification framework for NFC research.

Infrastructure with other categories. Moreover, NFC Infrastructure related research facilitates new business needs.

NFC Applications and Services is the other intermediate level which is influenced by the other three categories. The papers within this category provide a problem space or new business needs. NFC technology covers a wide range of applications that provide real implementations or prototypes with rigorous design artifact evaluations such as experimental, testing, field studies and so on. The papers in this category are also grouped according to the application's operating modes: "Reader/Writer Mode Applications", "Card Emulation Mode Applications" and "Peer-to-Peer Mode Applications". Indeed, design artifacts which propose applications or services operating in two or more modes can be seen in NFC literature.

The NFC Ecosystem is the highest level of the NFC research framework. This level is part of the problem space or environment of NFC research, the improvements or changes in the middle and fundamental layers affect NFC Ecosystem significantly. The papers within this category are grouped under "NFC Economics and Strategy", "NFC Business Models and Processes" and "NFC Stakeholders, Structure and Culture". The first two groups deal with the business requirements, analysis and managerial sides of the NFC technology. The third group deals with the social sides of NFC technology such as roles, characteristics and capabilities (e.g., user acceptance, usability, adoption, reliability, and manageability) of stakeholders (e.g., MNOs, service providers, and end users), and culture of NFC enabled services. Stakeholders play a crucial role in facilitating NFC research and development. In an NFC ecosystem, the goals, tasks, problems, and

opportunities define business needs as they are perceived by the stakeholders. These perceptions are shaped by the roles, capabilities and characteristics of the stakeholders evaluated within the context of economics and strategies, structure and culture, and business models and processes.

(ii) *Evaluation of the academic review*

NFC as a new emerging research area has attracted the attention of both practitioners and academicians. As cited earlier, academic research activities in the NFC area have significantly increased since 2006. This literature review wants to shed light on the current status of NFC research. The results from the NFC classification scheme have several important implications:

- There is a clear need for more journal publications to provide business related and rigorous research papers on NFC technology.
- It is not surprising that most of the academic research papers are related to NFC Applications and Services, especially operating in reader/writer mode. The reason for such interest on this mode is that development and implementation of such services or applications are much easier than developing applications operating in other modes. Unfortunately there are only a few research papers on "Peer-to-Peer Mode Applications".
- Another large proportion of the papers are related to NFC Infrastructure. Our review shows the importance of focusing on technical issues of a new technology again, rather than issues related to realizing economics, business values or strategies for NFC development, dissemination, and marketing. More specific research study needs to be conducted on business issues, and economics of NFC technology.
- When developing a NFC service, the ecosystem and business environment of that NFC service need to be considered as well. Such new applications can bring new business models and processes with new players. In particular, the capabilities, characteristics and roles of stakeholders need to be evaluated and modified when necessary, in order to satisfy the requirements of new business models and processes. Cultural differences on adopting NFC enabled technologies could be an interesting area for investigation.
- Policy, ethical and legal problems which can be referred to as behavioral issues were other important and demanding research areas for development of a new, emerging technology. However, it is hard to find papers dealing with the public policy and legal problems (e.g., taxation problems, trust, fraud, privacy issues for Internet privacy, and financial privacy). Indeed, this should prompt academicians to investigate this area.
- Today it seems that the most popular NFC related research areas are on developing new NFC enabled applications and developing NFC infrastructure. Thus, NFC research can be mostly referred to as design science research that proposes innovative artifacts and provides utility for relevant business problems. In the meantime, utility and efficiency of the proposed artifact must be demonstrated in well-defined methods. Most of the papers use more descriptive (e.g., scenarios, and use cases to demonstrate its utility) or analytical (e.g., architecture analysis) methods while developing an application or service, rather than performing experimental and testing methods. In some papers, inadequate design evaluations are performed, or implications of the proposed design artifacts are observed. Instead of evaluations through scenarios or use cases, field studies, controlled experiments, or simulations will be more useful for representing the proposed artifact rigorously.

(iii) *Further research in NFC*

The literature review presented in [6] aims to provide a holistic review and a comprehensive base for understanding of NFC research. In addition to the evaluations, some academic research questions for further research in NFC are proposed:

- Are there any public policies, regulations and legal standards for the development and adoption of NFC technology at the individual and corporate level?
- How are the required NFC standards developed from policy, regulations and legal points of view?
- What are the impacts on the adoption and acceptance of NFC applications on the user side?
- What are the possible implications of cultural differences on adoption of NFC technologies and new business opportunities?
- How can developments in NFC technology as an information technology tool be evaluated in terms of economic performance and economic decision rules?

1.13 Chapter Summary

NFC as a promising research and development area has attracted the attention of both academicians and practitioners in the last decade. NFC technology aims to simplify daily human life by a simple touch and in the very near future, people will be able to benefit from several services by using their NFC mobiles. They will be able to purchase goods and services, access hotel rooms, apartments or cars, configure Wi-Fi and Bluetooth settings, upload health related data to hospital monitoring systems, and so on.

The underlying layers of NFC technology follow globally accepted standards of ISO, ETSI, ECMA and so on as well as the specifications of industry pioneers. NFC Forum is the most crucial association in advancement of the technology.

Although interoperable sets of standards and specifications are currently available, there is still a lack of common understanding of the need for collaboration. Since the profit within the market is very big, companies are ambitious to share this profit. Hence this creates a strong rivalry among MNOs, financial institutions, transport authorities, IT firms and so on which affects the progress of NFC ecosystem and business models. Up to now, various NFC trials and usability studies especially in the payment and ticketing service domain have been conducted throughout the world. Some led to commercial launches whilst others did not, due to failing to generate consistent business models.

This chapter provides a good introductory knowledge on NFC technology from various perspectives including technical, business, usability, and so on. It also presents valuable academic studies on the benefits of NFC applications and the status of academic research in NFC literature.

References

[1] NFC Forum, http://www.nfc-forum.org/ (accessed 10 July 2011).

[2] Ok, K., Coskun, V., and Aydin, M. N. Usability of Mobile Voting with NFC Technology. Proceedings of IASTED International Conference on Software Engineering, Innsbruck, Austria, 16–18 February 2010, pp. 151–158.

[3] Jaring, P., Törmänen, V., Siira, E., and Matinmikko, T. Improving Mobile Solution Workflows and Usability Using Near Field Communication Technology. Proceedings of the 2007 European Conference on Ambient Intelligence, Darmstadt, Germany, 7–10 November 2007, pp. 358–373.

[4] Franssila, H. User Experiences and Acceptance Scenarios of NFC Applications in Security Service Field Work. Proceedings of the 2010 Second International Workshop on Near Field Communication, Monaco, 20–22 April 2010, pp. 39–44.

[5] Ok, K., Coskun, V., Aydin, M. N., and Ozdenizci, B. Current Benefits and Future Directions of NFC Services. Proceedings of 2010 International Conference on Education and Management Technology (ICEMT), Cairo, Egypt, 2–4 November 2010, pp. 334–338.

[6] Ozdenizci, B., Aydin, M. N., Coskun, V., and Ok, K. NFC Research Framework: A Literature Review and Future Research Directions. Proceedings of 14th International Business Information Management Association Conference on Global Business Transformation through Innovation and Knowledge Management, Istanbul, Turkey, 23–24 June 2010, pp. 2672–2685.