Handbook of Research on Mobility and Computing:

Evolving Technologies and Ubiquitous Impacts

Maria Manuela Cruz-Cunha
Polytechnic Institute of Cávado e Ave, Portugal

Fernando Moreira
Universidade Portucalense, Portugal

Volume I

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE

Hershey • New York

Senior Editorial Director: Kristin Klinger
Director of Book Publications: Julia Mosemann
Editorial Director: Lindsay Johnston
Acquisitions Editor: Erika Carter
Development Editor: Michael Killian
Typesetters: Michael Brehm, Casey Conapitski, Keith Glazewski, Milan Vrarich Jr. & Deanna Zombro
Production Coordinator: Jamie Snavely
Cover Design: Nick Newcomer

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Handbook of research on mobility and computing : evolving technologies and ubiquitous impacts / Maria Manuela Cruz-Cunha and Fernando Moreira, editors.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-60960-042-6 (hbk.) -- ISBN 978-1-60960-043-3 (ebook) 1. Mobile computing. 2. Wireless communication systems. I. Cruz-Cunha, Maria Manuela, 1964- II. Moreira, Fernando, 1969 Aug. 16-
QA76.59.H35 2011
004.165--dc22
2010036723

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 45
RFID and NFC in the Future of Mobile Computing

Diogo Simões
Movensis, Portugal

Vitor Rodrigues
Movensis, Portugal

Luis Veiga
INESC ID / Technical University of Lisbon, Portugal

Paulo Ferreira
INESC ID / Technical University of Lisbon, Portugal

ABSTRACT

RFID (Radio Frequency Identification) technology consists of a tag that can be used to identify an animal, a person or a product, and a device responsible for transmitting, receiving and decoding the radio waves. RFID tags work in two different modes: they wake up when they receive a radio wave signal and reflect it (Passive Mode) or they emit their own signal (Active Mode). The tags store information which allows univocally identifying something or someone. That information is stored in an IC (Integrated Circuit) which is connected to an antenna, responsible for transmitting the information.

An evolution of this technology is the Near Field Communication (NFC). It consists of a contactless Smart Card technology, based in short-range RFID. Currently, there are mobile phones with NFC embedded in such a way that they work both as a tag and as a NFC reader. These technologies will be widely available both in mobile phones and other devices (e.g. personal digital assistants, etc.) in the near future allowing us to get closer to a ubiquitous and pervasive world.

This chapter describes the most important aspects of RFID and NFC technology, illustrating their applicative potential, and provides a vision of the future in which the virtual and real worlds merge together as if an osmosis took place.

DOI: 10.4018/978-1-60960-042-6.ch045

INTRODUCTION

Technology is a term with origins in the Greek *technología* (*τεχνολογία*) — *téchnē* (*τέχνη*), 'craft' and *-logía* (*-λογία*), the study of something, or the branch of knowledge of a discipline (Encyclopedia Britannica, 2009). Applied to the human species, this concept deals on how we use knowledge of tools and crafts in order to control and adapt to our environment. Historically speaking, the technology has been present since the beginning of mankind, being fire or the wheel some of the most revolutionary technological discoveries ever.

Technology also refers to the collection of techniques, as the knowledge of how to combine resources to produce desired products, to solve problems, fulfill needs or satisfy wants. Throughout mankind's evolution, the term technology has been applied in various different ways, resulting in the creation of different technological areas, such as the industrial technology, the military technology, the medical technology and many others. All of the different technological areas have the same common purpose of improving processes or creating new products in order to enhance a specific area. Typically, these technological areas are the result of a specific need in a specific area.

One of the most recent technological areas is the communications technology, which came as a result of the necessity for mankind to being able to communicate securely, faster and globally. The telephone and then the Internet were important technological advances when speaking of communication, allowing people to communicate seamlessly and globally, using different means (voice, text, data, and multimedia content).

For Human kind, there are two main aspects that have proven to be determinant throughout times, which are ambition and realization. Every time a technological barrier is broken, we realize that something that was not possible before is now real and we realize that we still have not reached the limit in that technological area. When we realize that, our ambition motivates us to overcome the next technological barrier. This is how information and communication technology has been evolving so rapidly during the last few decades.

Some years ago, we became able to communicate from one side of the world to another and this achievement created another need: being able to communicate in the same seamless and global way at the same time we could be mobile. This was how a new technological area was created, the Mobile Technology. The necessity of being able to communicate anywhere, anytime and at any speed has turned out into a major revolution in our everyday lives, and we are now able to use most of the communication technologies even while we are moving, by using the mobile phones which integrate those technologies.

This chapter presents how the Mobile Technology changed people's everyday lives and how it is on the verge of doing it again. In addition, we provide a practical scenario (based on a prototypical example called OSMOSIS) that illustrates the range of possibilities that are made possible by RFID/NFC technology.

Mobile Technology: Past Generations and Evolution

Nowadays, we are living in a new era, where everything and everyone is connected, at all times, anywhere. It is possible to be connected anywhere only due to the major technological evolution we have seen in the mobility and ubiquity areas. For the end users, the mobile technology became real with the appearance of the first mobile phones, just a few decades ago. At first, these devices only allowed people to communicate with each other by voice and the network had gaps in its coverage. This soon changed and the development of the mobile technologies went through three different generations of evolution in only a few years.

Mobile devices capabilities went from analog, circuit switched voice-only traffic to a whole set of advanced services and large bandwidth data transfer, seamlessly integrating multimedia services

(audio and video streaming, video conferencing and mobile TV), Internet (web access, email and social networks) and location based services. The current state of the mobile technology represents its third generation (3G) and despite being extremely recent and with fast growing market with a set of services yet to be explored, the fourth generation (4G) is just around the corner and is expected to be launched in 2011 (Chennakeshu, 2008).

The fourth generation represents an enhancement of all the services integrated in the third generation by providing the means (up to 100Mbps download and 20Mbps upload data transfer speeds) for augmented and virtual reality to take place. Services such as interactive and High Definition mobile TV, full time online database access and any other services that were not possible to become mobile until the arrival of the 4G. WiMAX 802.16e, WiMAX 802.16m and LTE (Long Term Evolution) are the main technologies which will enable 4G functionalities. The commercial launch of these technologies, and the availability of compatible mobile devices, is expected to begin in 2010 or 2011 (Dekleva, Shim, Varshney, & Knoerzer, 2007).

Every Technology Wants Turn Mobile

Mobility and Ubiquity, despite being two different words, are closely related to each other when it comes to the mobile technology industry. Mobility, according to the American Heritage Dictionary, means "the quality or state of being mobile" while ubiquity is defined as "existence or apparent existence everywhere at the same time" (Shepard, 2003). Despite having different meanings, it is easy to understand how close they get when taking into account all the advantages the mobile technology has brought into our lives: the communication functionalities provided by mobile phones allows people to access almost any service from any place, independently of their geographic location and, at the same time, they are available in one of the most used and important personal objects that people carry in their pockets every day: the mobile phones.

Besides all the broadband technologies currently integrated into mobile phones, there are several other technologies that relate to the terms mobility and ubiquity. So, it is only natural that a global effort is being undertaken by many companies in order to integrate those technologies into the mobile phones and other devices.

Radio Frequency Identification

RFID, or Radio Frequency Identification, first appeared as a technology itself during the Second World War (Journal, RFID). This identification technology allowed allies to distinguish their airplanes from the enemy's by the response obtained from the reflection of radio frequency signals emitted into the air. Since then RFID has come a long way and has conquered areas other than the military, becoming part of our everyday lives in several different areas. RFID enhances convenience and productivity and, for that reason, is applied to theft prevention, toll payments without the need to stop, traffic management, access control for people and automobiles, asset tracking and monitoring, mobile payments, supply-chain and warehouse management, and many other areas (AIM, Inc., 2001).

Basically, RFID technology consists of a tag identifying an animal, a person or product and a device responsible for transmitting, receiving and decoding the radio waves. RFID tags work in two different modes: they wake up when they receive a radio wave signal and reflect it (Passive Mode) or they emit their own signal (Active Mode). The tags store information which allows univocally identifying something and someone. That information is stored in an IC (Integrated Circuit) which is connected to an antenna, responsible for transmitting the information.

Despite all of its possible applications, Radio Frequency Identification also has some disadvantages, like (Barata Simões, 2008):

- Interference between the signal of two or more different receivers, resulting in incorrect responses by the tags to the different read requests;
- It may be difficult for the receivers to read too many different tags in a determined area. This conflict can be overcome by sending one read request at a time;
- The data stored by the RFID tags is static, so all the information computation is done by the receivers.

The advantages which justify all the different RFID's applications are:

- The possibility to univocally tag every item with its own specific information;
- Being able to define Read/Write permissions for every tag;
- The information can be exchanged between the tags and the receivers without the need for them to be in contact with each other. The maximum communication distance depends on the frequency and on the power used by the RFID system.

There are three different types of RFID tags: the passive, the active and the semi-passive. Only the passive and the active tags present relevant differences, since the semi-passive ones are a hybrid of both. The tags differ in the way they receive power for transmitting information: the active tags integrate their own power source (i.e. battery) allowing them to send information without a receiver having requested it, while the passive tags draw the power for transmitting information from the electromagnetic waves transmitted by the receivers. In some cases, the passive tags are able to store some power for sending a quick response a short while later. Active tags present another advantage against the passive ones which is their range of 300 feet or more. The passive tags need a great amount of power for sending a short and low-powered answer to the receiver, resulting in a very short range (from approximately 4 inches to 10 feet, depending on the frequency used). Table 1 presents a comparison between both the active and the passive RFID modes.

The range of a RFID system depends on the frequency used by it. When combined with the active and passive modes, the result is a field with a range that can go from under 10 inches to hundreds of feet. Frequency refers to the cycle rate (and associated wavelength) of the radio waves used to communicate between the RFID tags and the receivers. Despite the direct equation between

Table 1. Technical and functional differences between active and passive RFID modes (Technology, Savi, 2002)

	Active	Passive
Tag Power Source	Internal	Transferred from the receiver by RF
Battery	Yes	No
Energy Availability	Continuous	Only if under the receiver field
Required Signal Strength (Receiver → Tag)	Low	High (must be enough for providing energy to the tag)
Generated Signal Strength (Tag → Receiver)	High	Low
Communication Range	Long Range (300 feet or more)	Short Range (10 feet or less)
Multi Tag Read	A single receiver is able to communicate with thousands of tags within a range of dozens of feet	A single receiver is able to communicate with hundreds of tags within a range of 10 feet
Data Storage Capacity	High Capacity	Low Capacity

a higher RFID frequency and faster data transfer rates and longer read ranges, environmental factors must also be taken into account, such as liquid, metal or walls that can interfere with the radio waves propagation.

Taking into account all the variables (range, data transfer rates and environmental factors) is strictly necessary when implementing a RFID system. For instance, a higher frequency system is equivalent to faster data transfer rates and longer read ranges, but is also equivalent to decreased capabilities in reading near or on liquid or metal surfaces. It is very important to understand that there is no ideal frequency for all applications, even within a single industry.

Currently, RFID can operate in the Low Frequency (LF), High Frequency (HF) and Ultrahigh Frequency (UHF) bands. The different bands are exposed in Table 2 (Ward, van Kranenburg, & Backhouse, 2006).

Smart Cards

The Smart Cards are quite a recently technology that has been introduced in Europe just about a decade ago. This technology was born from a partnership between Motorola and Bull (Shelfer & Procaccino, 2002). The main advantages provided by this technology are:

- Increased convenience and security in a transaction;
- Tamper-proof identity information storage;
- Increased security in a system that may have data storage security failures or external attacks;
- Computational Power allowing to execute in-card operations;
- Great storage capacity.

Smart Cards have almost an unlimited number of possible applications such as (Cross, 1996):

- **Credit Card:** Electronically extended credit for transactions
- **Debit Card:** Allows users to access money, typically in a POS (point-of-sale) or ATM, after inserting a PIN;
- **Stored Value Card:** This is the first step for a society without physical money. A fixed value is electronically stored in the card. Sellers can transfer the value directly from the card to their account by using a proper reader. These card can be recharge-

Table 2. RFID frequency comparison

Frequency Band	Description	Operating Range	Applications	Benefits	Drawbacks
125 KHz to 134 KHz	Low Frequency	< 1.5 ft.	• Access Control • Animal Tracking • Product Authentication	Works well around water and metal products.	Short read range and slower read rates
13.56 MHz	High Frequency	< 3 ft.	• Smart Cards • Smart shelve tags for item level tracking • Library Books • Airline Baggage	Low cost of tags	Higher read rate than Low Frequency
860 MHz to 900 MHz	Ultrahigh Frequency	9 ft.	• Pallet Tracking • Electronic Toll Collection • Parking Lot Access	EPC Standard built around this frequency	Does not work well around items of high water, liquid or metal content
2.4 GHz	Microwave	3 ft	• Airline Baggage • Electronic Toll Collection	Fastest read rates	Most Expensive

able, disposable or automatically unusable after their stored value reaches zero;
- **Identification Card:** Securely stores personal information (biometric data, usernames and passwords, medical information, etc.);
- **Loyalty Card:** Stores accumulated points or credit that can be changed for some kind or reward, by its owner (coupons, discounts, products, services, etc.);
- **Ticket:** Stores information which grants access to some kind of event or infrastructure (concerts, public transportation networks, etc.).

A Smart Card consists of an Integrated Circuit (IC) embedded into a plastic card. The IC can be a microcontroller (CPU/MPU), with an internal memory chip and controlled by an Operating System, or just a plain memory chip. The main difference between the two kinds of ICs is that the one with a microprocessor allows adding, erasing and manipulating the information it stores, while the other one can only perform predefined operations (Farrell, 1996).

One of the main advantages of Smart Cards is the fact that one single Smart Card can store several different applications. For instance, the same Smart Card could be used as an Identification Card, as a Stored Value Card, as a Loyalty Card and as a Public Transportation rechargeable card, each application with its own security mechanism.

Besides integrating or not a microcontroller, a Smart Card can differ from other Smart Card in its communication mechanisms: it can have a contact or a contactless communication interface. The latter draws energy as passive RFID tags do, through the electromagnetic field created by the reader.

Data Exchange Format: ISO/IEC 7816 and ISO/IEC 14443

The Smart Cards depend on well established and defined standards for exchanging information with the readers. The ISO/IEC 7816 is an extension of ISO/IEC 7810 which defines four formats for the physical characteristics of identification cards. ISO/IEC 7816 has fifteen different parts, but only the fourth is presented since we focus only in contactless Smart Cards.

The ISO/IEC 7816 – Part 4 specifies the security, the organization and the commands for exchanging data. Accordingly to this standard, the data is exchanged by using APDU (Application Protocol Data Unit) commands. An APDU command is divided into a mandatory header and an optional body. Tables 3 and 4 present the structure of an APDU command and the meaning of each parameter, respectively.

Table 5 and Table 6 present the structure for a response APDU command and its parameters specification.

The ISO/IEC 14443 is the international standard for "Identification Cards – Contactless Integrated Circuit Cards – Proximity Cards" and was originally developed for electronic money and ticketing (Smart Card Alliance, 2002). Nowadays, it is used for any other applications capable of using a contactless Smart Card. The ISO/IEC 14443 relies on RFID for establishing communication and uses HF RFID (13.56 MHz), supporting two different communication protocols: Type A and Type B. This frequency was not only chosen because of its efficient induction

Table 3. APDU command structure (ISO/IEC, 2005)

APDU Command						
Header (Mandatory)				**Body (Opcional)**		
CLA	INS	P1	P2	[Lc Field]	[Data Field]	[Le Field]

Table 4. Command APDU specification (ISO/IEC, 2005)

Code	Name	# Bytes	Description
CLA	Class	1	Class of the Instruction
INS	Instruction	1	Code of the Instruction
P1	Parameter 1	1	INS qualification, or for input data
P2	Parameter 2	1	INS qualification, or for input data
[Lc Field]	Length	From 1 to 3	Length (bytes) of the [Data Field]
[Data Field]	Data	Same as Lc	Byte Array with the command data
[Le Field]	Length	From 1 to 3	Maximum length (bytes) of the [Data Field] in the response APDU

proximity coupling but also because of its low absorption levels by human tissue through the skin.

Nowadays, it is demanded by all the entities total compatibility with all the four parts of the standard for both the cards (PICC – Proximity Integrated Circuit Cards) and the readers (PCD – Proximity Coupling Device). VISA and MasterCard have already included this ISO in their contactless specifications.

Although it defines a protocol supporting reliable data transmission with multiple cards, the ISO/IEC 14443 does not define the data format. Instead, it relies on the ISO/IEC 7816 – Part 4. This fact guarantees the ISO/IEC 14443 backward compatibility, justifying any investment in Smart Cards, whether they are contact or contactless.

MiFare is the open-source standard (developed by Philips and currently regulated by NXP Semiconductors) leader of the industry for transactions relying on Contactless Smart Cards (NXP Semiconductors, 2009). This standard is no more than a coding/authentication protocol for Contactless Smart Cards in accordance with the ISO/IEC 14443 – Type A specifications. MiFare is considered to be a de facto standard by the industry and is used as a comparison for any new contactless standard. The MiFare Interface Platform has six different products in its family (NXP Semiconductors, 2009):

- **MiFare Classic:** Integrated Circuits (IC) which use the communication protocol MiFare (standard MiFare 1K e 4K);

Table 5. Response APDU command structure (ISO/IEC, 2005)

Response APDU		
Body (Optional)	**Trailer (Mandatory)**	
[Data Field]	SW1	SW2

Table 6. Response APDU command structure (ISO/IEC, 2005)

Code	Name	# Bytes	Description
[Data Field]	Data	Variable	Byte Array with the response data
SW1	State 1	1	Processing state of the command
SW2	State 2	1	Qualifier for the command processing

- **MiFare Ultralight:** Developed with the main objective of being inexpensive and to fit in a paper ticket. Present a viable alternative to the existing magnetic stripe tickets.
- **Double Interface Controllers:** Includes the MiFare PRO and the MiFare PROX, providing flexibility and security in order to support multiple applications in the same IC.
- **MiFare DESFire8:** First contactless IC to support AES (Advanced Encryption Standard) as well more common standards such as DES and 3DES.
- **Reading Components:** Readers and evaluation kits in compliance with the contactless standards like the ISO/IEC 14443 A/B and the ISO/IEC 15693.

MiFare

On March 2008, the MiFare team of the Digital Security Group of the Radboud University Nijmegen revealed a security vulnerability in MiFare Classic RFID chips, the most commonly used type of RFID chip worldwide, that affects many applications using Mifare Classic (Digital Security Group, 2008). This "hack" could have major implications and NXP Semiconductors, which had previously been notified by the "hackers", had already started a new specification for solving this flaw.

FeliCa

Like MiFare, FeliCa is a standard for contactless ICs and was developed by Sony Corporation. This standard was broadly adopted in many Asian countries, in areas such as transportation ticketing and electronic payments. As a matter of fact, FeliCa may be seen as the "Asian" equivalent to the "European" MiFare.

This standard relies on a proprietary communication protocol and is compatible with 212 Kbps (passive communication mode of ISO 18092).

Near Field Communication (NFC)

Near Field Communication is an emergent technology focused in contactless short range connectivity. This technology evolved from the combination of other contactless identification and communication technologies, turning the connectivity between electronic devices into something much easier. By enabling simple and secure bidirectional interactions between electronic devices, NFC allows users to do secure contactless transactions, provides seamless access to digital content and allows devices to connect with a simple touch (Cassidy, 2007). As a result, NFC increases the comfort, the security and speed in several different processes such as moneyless payments, buying tickets using the mobile phone at anytime and anywhere, better loyalty services, and centralization of your cards in your phone and many other functionalities and services.

Initially, NFC appeared as a result of an effort taken by Royal Philips Electronics and Sony Corporation. In 2004, these two companies created the NFC Forum in order to promote the implementation and definition of NFC as a standard so that it would guarantee a future interoperability between devices and services. At this moment, NFC Forum has approximately 150 members and is still the reference in the expanding NFC ecosystem.

NFC consists of a contactless Smart Card technology, based in short-range HF RFID which operates at 13.56 MHz. Not only does NFC present backwards compatibility with the existing contactless standards, but it also implements two proprietary standards: the NFCIP-1 and the NFCIP-2. This technological merge and compatibility allows the same technology (the Near Field Communication) not only to emulate a contactless Smart Card, but also to work as a RFID reader or as a RFID tag. The latter mode presents NFC

as a very appropriate technology for devices identification and communication initialization.

NFC may operate in three different modes and is based on two different contactless standards: ISO/IEC 18092 NFCIP-1 and ISO/IEC 14443. The three modes are the following (Figure 1) (NFC Forum, 2009):

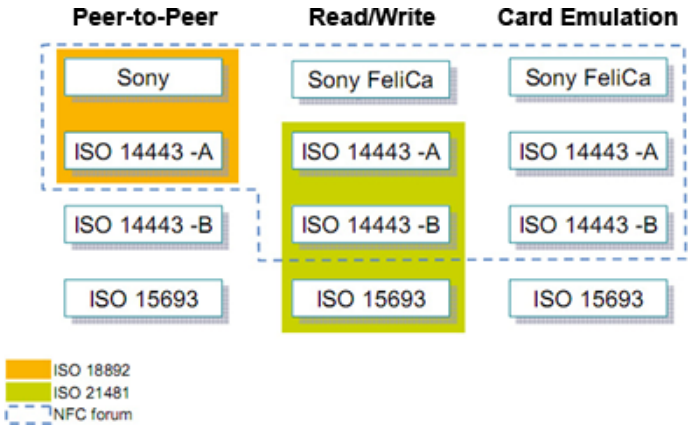
- **Read/Write Mode:** the NFC device is able to read NFC RFID tags or to act as one. This mode has a Radiofrequency interface in compliance with ISO/IEC 14443 and FeliCa;
- **Peer-to-Peer Mode:** two NFC devices are able to establish a bidirectional communication for exchanging data. For instance, it can share Bluetooth or Wifi connection parameters, or they can exchange data like business cards or digital photos. This mode is in compliance with ISO/IEC 18092;
- **Card Emulation Mode:** the Secure Element chip allows the NFC device to act as a contactless Smart Cards, providing the same functionalities.

As it was stated in the beginning of this chapter, the mobile phone has turned into a "whole-in-one" device, providing communication technologies that underline both the mobility and ubiquity concepts while being most people's "number one" personal object. For this, mobile phone was elected as the ideal device for bringing NFC to the end user.

A NFC mobile phone has three main components, which are:

- **Antenna:** allows the generation of the electromagnetic field used for transmitting data;
- **NFC Chip:** manages the communications between the application processor of the mobile phone, the antenna and the place where the secure applications (i.e. applets) are stored (Secure Element);
- **Secure Element:** component responsible for storing applications or data with high security requisites. The Secure Element architecture consists of a Java Card area, a MiFare area and a FeliCa area. The applets are the Smart Card Applications which are installed into the Java Card area and use the Java Card CPU for processing information. MiFare and FeliCa are authentication and codification standards for contactless Smart Cards which store information statically in their dedicated memory area. Each of the three components of the Secure

Figure 1. NFC Communication Modes (Brun, 2007)



Element are protected from the exterior and from them by a firewall.

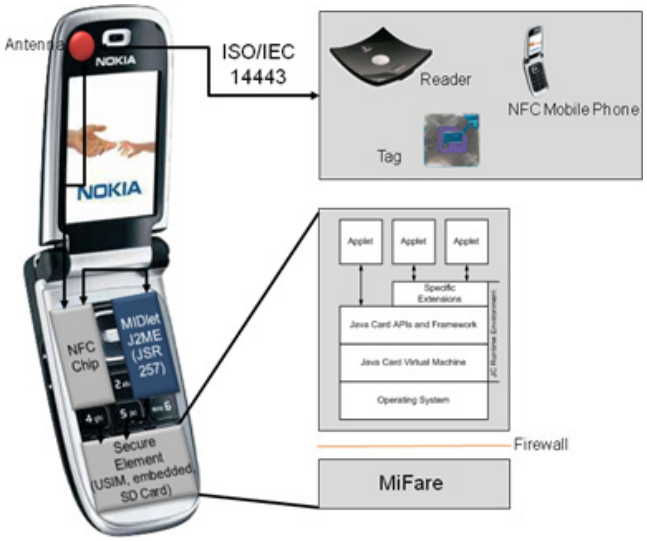
The Secure Element (SE) may be seen as the place, in a NFC mobile phone, where any data requiring security is stored. In the SE there can be stored several applications, operating independently between themselves and independent from the phone itself. This has been the most undefined area of NFC for quite some time since the location of the Secure Element chip was yet to be defined (Giesecke & Devrient GmbH, 2009). However, on May 2008, ETSI (European Telecommunications Standards Institute) specifications defined that the location of the Secure Element should be in the (U)SIM. Despite being recognized by ETSI, the Element Secure can actually exist in three different places which are:

- **(U)SIM:** the communication between the NFC chip and the Secure Element present in the (U)SIM (Universal Subscriber Identity Module or Universal SIM) is done through the SWP (Single Wire Protocol). The SWP is the specification for establishing a connection between the Secure Element and the NFC chip using only one contact of the (U)SIM contact interface. The (U)SIM based Secure Element allows the applications to be portable between NFC devices and an easier and more centralized component in case of theft or damage of the SE. At the same time, this centralization can also be negative, since all the applications OTA (Over-the-Air) provisioning has to go through the operators;
- **Mobile Phone embedded chip:** this solution does not present any particular aspect regarding the communication between the NFC chip and the Secure Element, since they are both embedded into the same system;
- **Flash Memory Cards:** despite allowing application to be portable and device independent, this solution seems to be in an inferior evolution state. Recently, some solutions brought to market and certified as secure by VISA and MasterCard revived this kind of solutions.

NFC Ecosystem

For the last two years, NFC has struggled to reach the market with no success. It was not a failure but a delay, since every player of the NFC ecosystem

Figure 2. NFC Mobile Phone Architecture (Barata Simões, 2008)



recognizes the value and bright future of Near Field Communication. But now, with the SWP protocol being recognized by ETSI specifications, the NFC players are finally organizing themselves and deciding which part they want to take.

The NFC ecosystem can be basically reduced to three different parts (Cox, 2009):

- **MNO:** The Mobile Network Operators (MNO) "won" the war against mobile phones manufacturers. They are now the only channel possible for remote installation and management of the applets (i.e. Secure Element's applications), since the Secure Element is embedded into the (U) SIM which is owned by the MNOs;
- **SP:** The Service Providers (SP) is clearly the weakest part of the ecosystem but also the one where there will be more competition. Any entity that wishes to implement an NFC service that requires an application to be installed into the Secure Element is a Service Provider and can only get a business model by providing that service to its clients, remotely, relying on the MNOs infrastructure to do so;
- **TSM:** The Trusted Service Manager (TSM) presents itself undoubtedly as a candidate to the major part in the NFC ecosystem. A TSM will be the central part which allows connecting every participant: if a SP wants to launch a new NFC service and install a new applet into the Secure Element of its client's phone, he has to deal directly with the TSM. The TSM, which already has connections with all the MNOs, guarantees the whole path from the SP, through the MNOs into the mobile phones. This path allows TSM to securely distribute provision and manage the life cycle of NFC applications to the customer base of mobile network operators on behalf of service providers.

Each part has already many interested players, and the division is becoming type based. The MNO's part is being taken by the MNO, obviously. The SP part is being taken by every service provider that depends on innovation, such as transportation companies, retail brands, major franchising networks and any other entities with a harsh market, where innovation represents more clients. Finally, the TSM part is being taken by some NFC expert companies, but mostly by the (U)SIM manufacturers, which can easily position themselves as TSMs since they have the complete know-how and required access to the Secure Element.

Regarding TSMs, there are different opinions about which companies will be able to play a role as a Trusted Service Manager. At the moment, the general opinion is that only the biggest players in the NFC market, such as the (U)SIM developers and suppliers or the actual card issuers will be able to position themselves as TSMs in the NFC ecosystem. This point of view is supported by the fact that if a company wants to play a role as a TSM, it will be totally necessary for that company to keep ongoing contacts not only with all the service providers but also with all the Mobile Network Operators. This task presents itself as an extremely difficult one, if we take into consideration the fact that many Service Providers are part of very specific and hard to reach markets like financial or military ones.

Although the actual TSM reality suggests that in the future there will be just a few global TSMs, this might not be true. Smart Card technology may be applied to practically almost any market and every market has its own requisites like security, storage, communication or frequency. Thus, it is legit to think that TSMs will not only be distributed not only by region, but also by specific market areas. For instance, the military or the financial institutions present much more security requisites than loyalty or ticketing institutions.

NFC Case Studies Example

The NFC technology represents an evolution which enables applications such as payments, loyalty programs, ticketing, content distribution, device pairing and many others to be fully centralized in our mobile phones without changing the actual infrastructure.

The following diagrams represent some practical applications where the NFC technology can be used.

Figure 3 represents a practical example of how the acquisition of a service would be locally activated and remotely installed into the end user NFC mobile phone's Secure Element, through the mobile network. In this example, the service is considered to be a secure applet, either it is Java Card, MiFare or FeliCa. In the presented situation, the End User needs to activate a specific NFC service (for instance, a NFC loyalty card). First, the user must go to a Client Support Counter that represents the entity providing the loyalty service and request its activation. The Client Support Technician then notifies the Service Provider (SP) infrastructure of the need to send the new loyalty card applet. The SP gives authorization to the Trusted Service Manager (TSM) to proceed with the applet's installation. The TSM uses the Mobile Network Operator's network to conclude the process by installing and personalizing the loyalty card applet for the specified End User.

A Smart Poster is an NFC component which allows, through a specified format, to initiate several different services in an NFC mobile phone, such as sending a SMS with predefined data and recipient, making a call to a predefined number, initializing the phone's web browser in a predefined website and many other services. These functionalities give the possibility of using the NFC technology as a driver for initiating other services such the request for a remote installation of an applet (i.e. loyalty card, ticket, etc). Image 4 represents one of such situations. Taking the same example described in Figure 3, the End User who needs to activate a loyalty service by acquiring the NFC loyalty card, instead of going to a Client Support Counter, just has to touch a Smart Poster advertisement to initiate the activation of the loyalty service. The Smart Poster immediately initiates the sending of a pre-defined SMS for the entity pre-defined recipient. The SMS represents a request for the installation of the entity's loyalty card into the End User NFC mobile phone. The rest of the process is exactly the same one represented in steps 3, 4 and 5 of the previous example (Figure 3).

The example represented in Figure 5 is very similar to the one represented in Figure 3. The only difference is the fact that the NFC service for which is being requested the installation of the applet has an associated cost. In this example, the

Figure 3. Acquire Applet Locally (Payment Not Required)

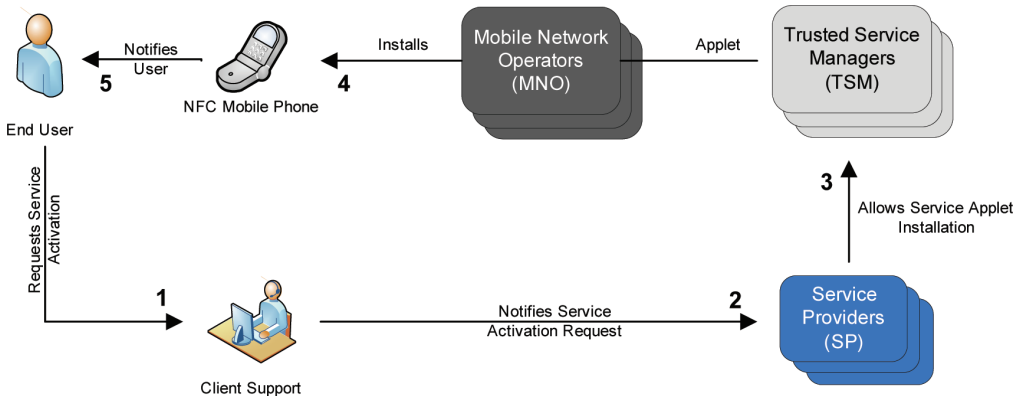
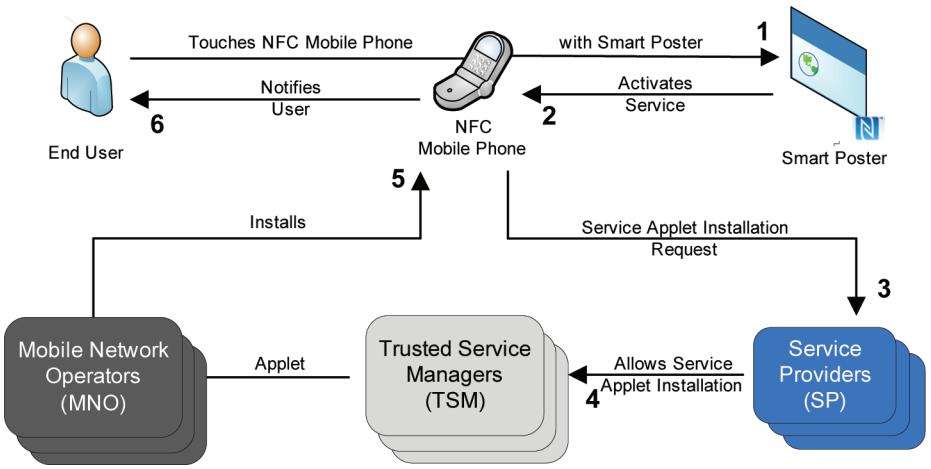


Figure 4. Acquire Applet using Smart Poster (Payment Not Required)



service could be, for instance, the acquisition of a ticket for a certain event. Steps 1 to 4 are the only difference between this example and the one represented by Figure 3. In Figure 3 the service did not require any previous payment, while this example requires a payment for the service (the ticket, for instance) before it can be actually installed into the phone. Steps 3 and 4 represent the confirmation for the payment which is necessary for the rest of the process to take place. After these steps are successfully concluded, the remote installation of the ticket into the End User's NFC mobile phone Secure Element is done in the same way as the NFC loyalty card was installed in the two previous examples.

Regarding the example represented in Figure 6, the process is analogue to the one represented in Figure 4 except for the fact that the payment has to be done remotely. This remote payment can be accomplished by a pre-defined SMS sent either to the Service Provider (SP) or to the entity responsible for regulating services payments, through a Mobile Banking SMS-based system. The latter solution is only possible if the End User has the Mobile Banking service previously activated.

The first four examples represent different ways to acquire a NFC service, be it a loyalty card, an event ticketing or a stored-value payments card. In Figure 7, the End User could have already

Figure 5. Acquire Applet Locally (Payment Required)

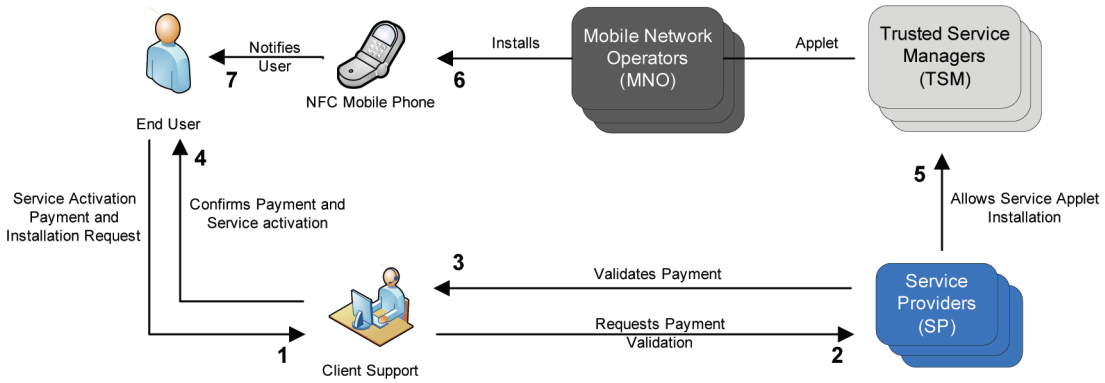
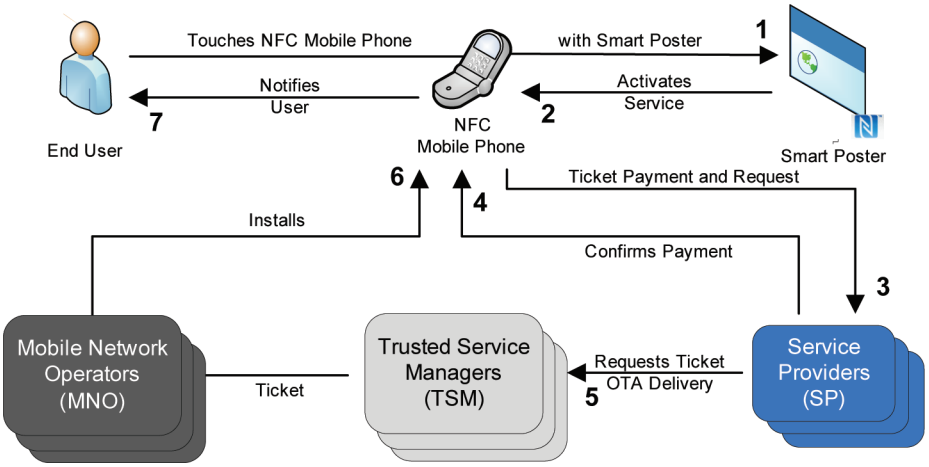


Figure 6. Acquire Applet using Smart Poster (Payment Required)



installed a NFC loyalty card for a specific entity and a stored-value payments card. After having both solutions installed, lets imagine that the user wants to pay something in a gas station and that the NFC loyalty card installed is the one of the gas station company. In this situation, the user would only have to touch the NFC reader connected to the entity POS and, instantly, the cost of the shopping would be debited from the stored-value card at the same time the loyalty points would be credited into the NFC loyalty card.

As it was described while presenting the first four examples, the NFC technology can also be used to securely acquire and store tickets for events, public transportation or any other access control system. The diagram presented in Figure 8 represents the practical case of consuming a previously acquired ticket. The End User just has to select the right ticket, touch the NFC area in the access control device and the system automatically grants access to the user, after validating and consuming the ticket. After this, the ticket no longer exists in the NFC mobile phone Secure Element.

All the diagrams previously presented have high security requisites, thus are all dependent of

Figure 7. Grant/Debit Points or Credit

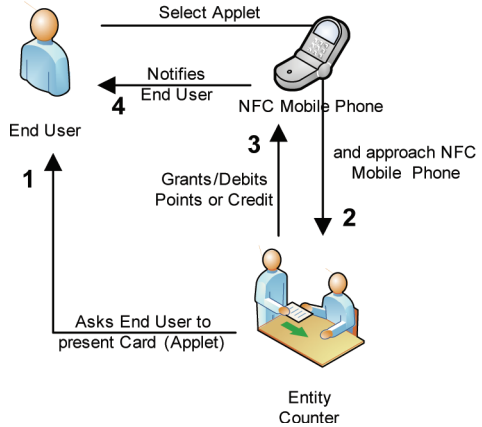
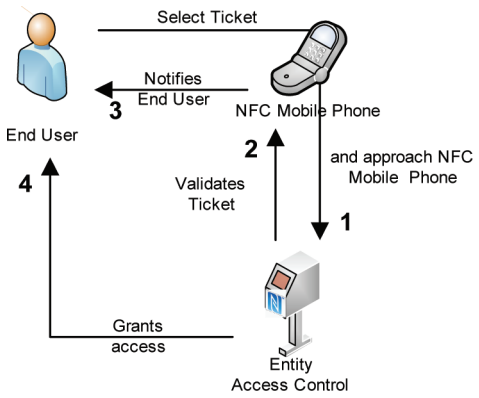


Figure 8. Consume Ticket



the Secure Element component. However, there are other applications for the NFC technology that do not need to use that component. One example is content distribution, which is represented in the following two diagrams (Figure 9 and Figure 10).

The content distribution is one of the applications where NFC has some limitations, since the NFC tags can store very few data. This limitation can easily become a bottleneck, since a NFC tag cannot store much more than a text and an image. The data transfer is as simple as touching a NFC Tag with the NFC mobile phone. This example is represented in Figure 10.

Figure 9 represents the alternative for when the data cannot be all stored in the same NFC tag. In this case, a NFC reader is used. The reader is connected to a Content Server which sends the content data to the NFC Mobile phone, through the NFC reader and using the NFCIP-1 as the communication protocol.

The NFC technology can be applied to many other applications such as pairing Bluetooth or WiFi devices or transmitting data between two NFC devices (photos, contacts, videos and many other).

A Prototypical Example: OSMOSIS

In this section, we present a prototypical example of a RFID/NFC-based middleware system that could very well become dominant in most homes. OSMOSIS serves to illustrate a ubiquitous middleware system that can be used at home or at the office by non-computer experts, on a daily basis, providing a number of answers and notifications to users concerning real-world objects. To operate, such a system requires the following:

- Insert real objects into the virtual world by attaching passive RFID tags to them, allowing the acquisition of their identification and location.

Figure 9. Content Distribution (NFCIP-1)

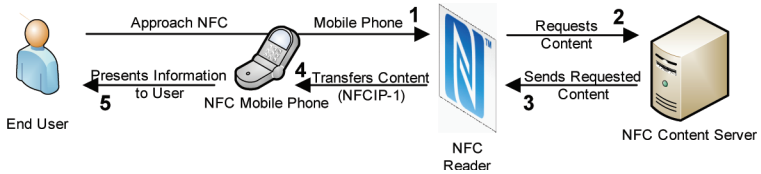
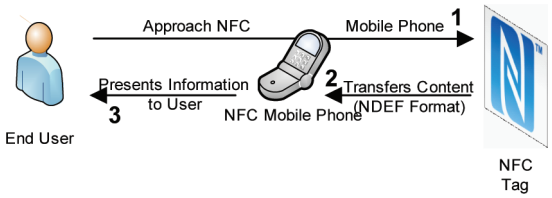


Figure 10. Content Distribution (NFC Tag)



- Offer a simple (as invisible as possible) user interface so that non-experts users can interact with OSMOSIS applications in a non-disruptive way.
- Provide a context-aware file system, offering traditional file-system API to develop applications, supporting context-information (e.g. object's location and history) associated to such virtual objects.

In OSMOSIS, real objects are associated with virtual objects represented by files. Creating a file as a counterpart of a real-world object has evident advantages, since it allows extending features and operations available in the virtual world to real objects. We can foresee several scenarios in which such an extension is useful as it enables users to answer common everyday questions as well as being notified of certain situations:

- Warn user if object x and y get close to each other.
- Warn a user if a child is close to some dangerous object x.
- Notify the user that she should take object x whenever she takes object y.
- Where is the object brought from the last summer vacations?
- What was the present given by Jane on my last birthday?

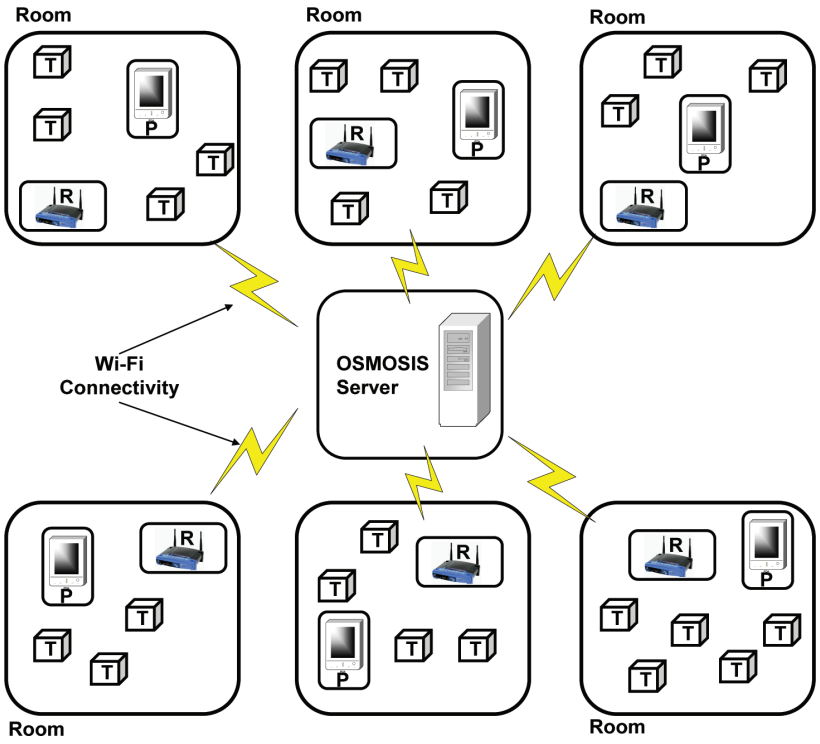
Such examples portray common situations that could be handled once we extend common operations performed on virtual objects (i.e. files) to real-world objects, and consider the additional context information associated with them. This allows the following: 1) search operations may be performed on disk data encompassing real-world objects that have been previously incorporated into the virtual world; 2) a user may be provided with information concerning which real-world objects should be kept together or near-by (once such objects are included in the virtual world), etc.

In Figure 11, we describe the organization of the physical entities involved in a house or office employing the OSMOSIS middleware. We conceive a house or office with a number of rooms, naturally connected via doors. A central OSMOSIS server is running on a desktop machine in any room (e.g., on the media center at home or at one of the office servers). Each room is equipped with a fixed RFID/NFC Reader that is able to detect and identify the tags associated with objects in the room.

In addition, users may use mobile devices which are NFC enabled, PDA or a mobile phone (e.g., Palm, PocketPC, IPhone, NFC-phone) that connects, via Wi-Fi, with the OSMOSIS server. With a PDA, users can make inquiries to the server (for instance, asking what objects are present in the room; where are other objects associated with a specific one, etc.) and receive notifications from the server (e.g., regarding forgotten objects when leaving the room).

Note that a PDA equipped with its own RFID/NFC reader could perform a close-range inspection lookingfor a specific object in a pile of objects (e.g., toys or briefcases). This NFC-reader capability enlarges the usage scenarios when compared to a situation in which there are only fixed

Figure 11. OSMOSIS Network Organization. Elements include RFID Tags (T), PDAs (P) and RFID Readers (R)



RFID readers. Obviously, the availability of NFC enabled devices, with reader capabilities, brings much more flexibility and power to the users. NFC-devices can also communicate with each other increasing even more the range of possibilities; in particular, by means of a synchronization process, such devices can exchange information that each one holds regarding, for example, the set of objects they are aware of, that are located in some room.

Naturally, for this scenario to succeed, all relevant objects in the real-world are tagged in order to be represented in the view the OSMOSIS server has of the complete surrounding environment. Regarding the current and forthcoming prices of RFID tags, namely passive ones, this is a feasible prediction of the near future.

Context and Semantic Information

In addition to specific information regarding objects, when employing a file system to represent the real-world objects, users may add context information to those files (e.g., explicitly appending text properties to files, or dragging file objects over others to state a contextual/semantic association among them, or grouping files together with the explorer application). Such semantic associations, once created, may be named (e.g., a category, a role), thus providing additional generic semantic and context information for the existing objects.

Since semantic associations are made explicit, they can be navigated as if virtual directories with a common file explorer application to visualize and navigate in the virtual world. Files are enrolled and removed from semantic associations based on context information available when they were first created, or other that has been added since.

Each semantic association can be presented as a virtual directory and the context menu regarding every file can be extended to include those associations that the file (and corresponding object in the real-world) is involved.

CONCLUSION

In this chapter we have exposed how technological evolution has been contributing to the solidification of the terms Mobility and Ubiquity. In the last few decades, we have seen that almost every emerging mobile technology was related to the improvement of the communication and its globalization. This fact was extremely important and we currently have several different technologies integrated into our mobile phones that allow us to be virtually anywhere, at any time, in contact with anyone, while moving and all of that in our pockets.

However, there are other technologies being explored and created at the same time that are focused in different areas than communication. Near Field Communication is a perfect example, where the mobile and telecommunications industry is making a global effort for establishing this emerging technology as a standard. Despite being an emergent technology, NFC is in fact, and generally speaking, a seamless and very useful integration of two different mature technologies: the RFID and the Smart Cards. By integrating a technology like NFC into the already broad set of communication technologies available in mobile phones, the mobile and telecommunications industry is taking a new step into a new definition of Mobility and Ubiquity. With this integration, not only are people able to be virtually anywhere at any time, but also their money and their assets become a part of that definition, allowing us to access mostly any service from our mobile phones.

Although we are still in a early stage for this new definition, it is expected that, with all the current efforts taking into action, peoples' everyday lives are on the verge of, once again, suffering an extreme improvement. End users just have to wait a little longer for this new reality.

REFERENCES

AIM, Inc. (2001). *Shrouds of Time - The history of RFID*. Pittsburgh: AIM, Inc.

Barata Simões, D. (2008). *Sistema de Fidelização sobre NFC*. Lisboa: Instituto Superior Técnico - Universidade Técniica de Lisboa.

Brun, M. (2007). *Exemples d'intégration de la technologie NFC*. NXP Semiconductors.

Cassidy, R. (2007). *Call For Entries Touching the Future: NFC Forum Global Competition*. Retrieved October 16, 2009, from NFC Forum: http://www.nfc-forum.org/news/pr/view?item_key=ffc0422bbc6504e4915ae500e4c19629dde0e5e9

Chennakeshu, S. (2008). *Technology Evolution of Mobile Devices. Stanford University, Networking Seminar*. Stanford: Stanford University.

Cox, C. (2009). *Trusted Service Manager: The Key to Accelerating Mobile Commerce*. First Data.

Cross, R. (1996, Abril 1). *Smart cards for the intelligent shopper*. (Direct Marketing) Retrieved Dezembro 10, 2007, from Allbusiness.com: http://www.allbusiness.com/marketing/direct-marketing/554240-1.html

Dekleva, S., Shim, J. P., Varshney, U., & Knoerzer, G. (2007). Evolution and Emerging Issues in Mobile Wireless Networks. []. New York: ACM.]. *Communications of the ACM*, *50*, 6. doi:10.1145/1247001.1247003

Digital Security Group. (2008). *Security Flaw in Mifare Classic*. Retrieved October 12, 2009, from Faculty of Science - Digital Security: http://www.sos.cs.ru.nl/applications/rfid/main.html

Encyclopedia Britannica. (2009). *Encyclopedia Britannica Online*. Retrieved October 20, 2009, from http://www.britannica.com/EBchecked/topic/585418/technology

Farrell, J. J. (1996). *Smartcards Become an International Technology*. Tokyo: IEEE Computer Society.

Forum, N. F. C. (2009). *Frequently Asked Questions - About NFC Technology*. Retrieved October 10, 2009, from NFC Forum: http://www.nfc-forum.org/resources/faqs/

Giesecke & Devrient GmbH. (2009). *Secure NFC*. Retrieved October 18, 2009, from Giesecke & Devrient GmbH: http://www.gi-de.com/portal/page?_pageid=42,127326&_dad=portal&_schema=PORTAL ISO/IEC. (2005). *ISO/IEC 7816-4:2005(E)*. Geneva: ISO/IEC.

Journal, R. F. I. D. (n.d.). *The History of RFID Technology.* Retrieved Novembro 17, 2007, from RFID Journal - The World's RFID Authority: http://www.rfidjournal.com/article/view/1338/1/129

Semiconductors, N. X. P. (2009). *MIFARE*. Retrieved October 5, 2009, from NXP Semiconductors: http://www.nxp.com/#/pip/pip=[pfp=53422]|pp=[v=d,t=pfp,i=53422,fi=,ps=0]|[0][0]

Shelfer, K. M., & Procaccino, J. D. (2002). Smart Card Evolution. [). New York: ACM, Inc.]. *Communications of the ACM*, *45*, 6. doi:10.1145/514236.514239

Shepard, S. (2003). *Mobility vs. Ubiquity: What Does the Customer Really Want?* Vermont: Shepard Communications Group.

Smart Card Alliance. (2002). *Contactless Technology for Secure Physical Access: Technology and Standards Choices*. New Jersey: Smart Card Alliance.

Technology, Savi. (2002). *Active and Passive RFID: Two Distinct, but Complementary, Technologies for Real-Time Supply Chain Visibility.* Savi Technology.

Ward, M., van Kranenburg, R., & Backhouse, G. (2006). *RFID: Frequency, standards, adoption and innovation*. Bristol: JISC Technology and Standards Watch.

KEY TERMS AND DEFINITIONS

NFC: A short range wireless RFID technology that makes use of interacting electromagnetic radio fields instead of the typical direct radio transmissions used by technologies such as Bluetooth. It is meant for applications where a physical touch, or close to it, is required in order to maintain security. The technology is promoted by the NFC-Forum.

NFC Ecosystem: A new market and technological ecosystem which resulted from the evolution of NFC and its specifications since 2006. This ecosystem has three major players that are the Mobile Network Operators (MNO), the Service Providers (SP) and the Trusted service Managers (TSM).

NFC Forum: The NFC Forum is a non-profit industry association that promotes the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs. Formed in 2004, the Forum now has 140 members.

OSMOSIS: A prototypical RFID/NFC-based middleware system where real objects are associated with virtual objects represented by files which allows extending features and operations available in the virtual world to real objects.

RFID: Method for identifying unique items using radio waves. Typically, a reader gets the information from the tag (tags can be passive or actively powered), which holds the unique information of the item.

Secure Element: The NFC architecture component responsible for storing applications or data with high security requisites. The Secure Element architecture consists of a Java Card area, a MiFare area and a FeliCa area.

Smart Cards: A credit card or other kind of card with an embedded microchip. When the card uses RFID technology to send and receive data it is called a contactless smart card.