

# Potential of Near Field Communication for Education

---

**Lamija Dzafic**





Lamija Dzafic, BSc

# **Potential of Near Field Communication for Education**

**MASTER'S THESIS**

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Software Engineering and Management

submitted to

**Graz University of Technology**

Supervisor:

Assoc. Prof. PhD Martin Ebner

Institute for Information Systems and Computer Media

Graz, September 2016

Contact:  
Lamija Dzafic  
lamija.basic@student.tugraz.at

## **EIDESSTÄTTLICHE ERKLÄRUNG**

### ***AFFIDAVIT***

I declare that I have authored this thesis independently, that I have not used anything other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or contextually from the sources used. The text document uploaded to TUGRAZonline is identical to the present master's thesis.

Ich erkläre an Eides statt, dass ich die vorliegende Arbeit selbstständig verfasst, andere als die angegebenen Quellen/Hilfsmittel nicht benutzt, und die den benutzten Quellen wörtlich und inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Das in TUGRAZonline hochgeladene Textdokument ist mit der vorliegenden Masterarbeit identisch.

## **Danksagung**

Ohne Menschen in meiner Umgebung, die mich immer wieder ermutigt haben endlich die Fertigstellung, nein, den Beginn meiner Masterthesis anzufangen würde es diese Arbeit wohl nicht geben. Gerade aus diesem Grund ist dieser Abschnitt der Arbeit, die Danksagung, mir sehr wichtig.

Mein erster und aufrichtiger Dank geht zunächst an meinen Betreuer Univ.-Doz. Dipl.-Ing. Dr. techn. Martin Ebner, ohne den diese Arbeit nie zu Stande gekommen wäre. Vor allem die Tatsache, dass ich ohne Druck arbeiten und mir die nötige Zeit nehmen konnte empfinde ich nicht als selbstverständlich.

Ein ganz besonderer Dank gilt auch meinem Ehemann, der während des Schreibens eine sehr große Entlastung war. Zu wissen, dass ich in jedem Bereich unseres Lebens auf dich zählen kann, ist wunderbar.

Zu guter Letzt gilt mein Dank meinen Eltern, die mir durch mein gesamtes Studium mit ihrer enormen Unterstützung geholfen haben. Diese Thesis ist zugleich auch ein Zeichen meines Respektes und meiner Liebe diesen zwei Menschen gegenüber. Hvala mama i tata.

## Kurzfassung

Near Field Communication bezeichnet eine Technologie die heutzutage hauptsächlich aus dem Bezahlsektor bekannt ist. Durch seine Verfügbarkeit auf Smartphones bietet NFC jedoch sehr viel Potential für eine Vielzahl von unterschiedlichsten Applikationen.

Diese Arbeit beschäftigt sich mit der Nutzung von NFC hinsichtlich aktueller aber auch zukünftiger Anwendungen. Verstärkt wird hierbei auch auf den Einsatz von NFC anstelle bereits verbreiteter ähnlicher Technologien eingegangen.

Um einen besseren Überblick über vergleichbare Technologien zu bekommen wird am Anfang der Arbeit auf den derzeitigen Stand der Technik im Bereich von kontaktlosen Technologien eingegangen. Da es sich bei NFC um eine Art Erweiterung der Radio Frequency Identification (RFID) handelt, wird ein besonderes Augenmerk auf diese Technologie gelegt. Auch optische Erkennungsverfahren, wie QR Code und Barcode, werden in dieser Arbeit hinsichtlich ihrer Vor- und Nachteile im Vergleich zu NFC erläutert.

Der praktische Teil der Arbeit beschäftigt sich mit der Nutzung von NFC im Bereich des spielerischen Lernens. Die Motivation war es mit der Methodik Prototyping eine Lösung für die Nutzung im Klassenzimmer zu finden, welche sowohl einfach, interaktiv als auch sinnvoll im Sinne von „Lernen durch Spielen“ eingesetzt werden kann. Das Resultat war eine Android-basierte Quiz Applikation mit dem Namen „NFCQuiz“ welche durch den Nutzen von NFC zum Zwecke des Datenaustauschs mehrere Spieler einbeziehen kann.

## Abstract

Near Field Communication is a technology that is known mainly through the payment and ticketing sector. Due to its availability on smartphones NFC provides a far untapped potential for a variety of different applications.

This thesis deals with the usage of NFC in actual and possible use cases. Especially its potential regarding the replacement of similar technologies is discussed.

First related technologies are introduced in order to get a better overview of the state of the art in the field of contactless technologies. Since NFC can be seen as an extension of Radio Frequency Identification (RFID), this technology will get special attention. Further optical recognition methods like QR Code and Barcode will be discussed with respect to their advantages and disadvantages regarding NFC.

The practical part of the work deals with the usage of NFC in the field of game based learning. The motivation was to test the potential and usability of NFC in educational area through the use of “prototyping” as solution strategy. The outcome of the research was an Android-based quiz application (“NFCQuiz”) using different NFC-approaches for data exchange.

## Contents

1	Introduction.....	10
2	Radio Frequency Identification (RFID).....	11
2.1	RFID-History.....	11
2.2	Auto-ID Center.....	12
2.2.1	Electronic Product Code (EPS).....	12
2.3	RFID-Infrastructure.....	14
2.3.1	RFID-Transponder.....	16
2.3.2	Communication Mode.....	26
2.3.3	RFID Reader.....	27
2.4	RFID Anti-Collision.....	33
2.4.1	Anti-collision protocols.....	34
2.5	How many tags can be read?.....	38
2.6	Security Requirements.....	39
2.6.1	Attacks.....	39
2.7	RFID applications.....	42
2.7.1	Supply Chain Management (SCM).....	42
2.7.2	Animal Identification.....	43
2.7.3	Budweiser’s buddy cup.....	44
2.7.4	Shopping with RFID.....	44
2.7.5	Burberrys RFID store.....	44
2.7.6	Electronic Road Pricing System (ERP).....	45
2.8	When is RFID the right solution?.....	46
2.8.1	RFID benefits for companies (Ferrer, Dew, & Apte, 2010).....	46
2.8.2	RFID problems and weaknesses.....	47
3	Near Field Communication (NFC).....	48
3.1	NFC-History.....	48
3.2	NFC Forum.....	49
3.3	NFC technology.....	50
3.3.1	Near Field Communication Interface and Protocol (NFCIP).....	51
3.3.2	Logical Link Control Protocol (LLCP).....	53



3.3.3	NFC Data Exchange Format (NDEF) .....	53
3.3.4	NFC Simple NDEF Exchange Protocol (SNEP).....	61
3.3.5	Tag Types .....	61
3.3.6	NFC operation modes.....	63
3.3.7	NFC with SoC and Microprocessor .....	76
4	NFC compared to other contactless Technologies.....	78
4.1	Barcode .....	80
4.1.1	Universal Product Code (UPC) .....	80
4.2	Quick Response (QR) Code .....	82
4.3	Smart Card.....	82
4.4	Popular use cases with respect to NFC.....	83
4.4.1	Tracking systems.....	83
4.4.2	Marketing .....	86
4.4.3	Entrance Systems .....	89
4.5	Comparison contactless technologies .....	90
5	Practical Part – NFCQuiz-App .....	92
5.1	Motivation .....	93
5.2	Android Basics .....	94
5.2.1	Android Manifest .....	94
5.2.2	Intent.....	95
5.2.3	NFC Adapter .....	97
5.2.4	Reading NDEF message from tag or beam .....	98
5.2.5	Writing NDEF message to tag or sending over beam.....	100
5.2.6	Host Card Emulation (HCE) .....	102
5.3	NFCQuiz guidance .....	107
5.3.1	NFCQuiz .....	108
5.3.2	NFCQuiz-Writer.....	119
5.3.3	Application examples .....	122
5.4	Discussion.....	125
6	Summary and Conclusion .....	127
7	Bibliography .....	129

8	List of Figures .....	135
9	List of Tables .....	138
10	List of Code Snippets .....	139

**List of Abbreviations**

ERP	Electronic Road Pricing System
HCE	Host Card Emulation
LLCP	Logic Link Control Protocol
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NFCIP	Near Field Communication Interface and Protocol
P2P	Peer-To-Peer
QR	Quick Response
RFID	Radio Frequency Identification
RTD	Record Type Definition
SCM	Supply Chain Management
SNEP	Simple NDEF Exchange Protocol
TDMA	Time Division Multiple Access



# 1 Introduction

This master thesis is dedicated to the topic Near Field Communication (NFC) – Potential for Education.

Even though NFC is not a new technology its distribution is still in its infancy. The reason therefor is probably the fact that the greatest potential of NFC is the replacement of already existing and more or less proofed technologies like QR Code, Barcode, Smart Cards, etc. This thesis deals with this potential from different points of view. The goal is to get an understanding for NFC, its advantages and disadvantages, especially in the field of usage. Beside the examination of NFC regarding already existing use cases the thesis tries to show up its potential in the field of education.

The progress that has been made in technology in the last decades has affected nearly every part of our lives. Although we have adopted this progress very well in economic and private area our educational system seems to have a lot to catch up. Technical equipment's like smartphone, computer and co. can be great helpers in teaching and learning environments. Especially a game-based approach can help to support the learning process in a funny and interesting way. Assuming this, the usability of NFC for education was investigated in this thesis. As a result a quiz game ("NFCQuiz") was developed through the use of "prototyping" pointing out some possibilities regarding its potential in the field of game based learning.

NFC can be seen as a sub part of Radio Frequency Identification (RFID). The fundamentals of RFID are mostly the same in NFC. Therefore Chapter 2 is describing RFID, its technical background, and popular use cases in detail. Subsequently Chapter 3 is devoted to NFC and its technical features. In Chapter 4 NFC is compared to the contactless technologies RFID, QR Code, Barcode, and Smart Cards.

The practical part of the thesis is described in Chapter 5. The already mentioned NFCQuiz is described regarding its implementation, functionality and possible use cases in education.

Finally, Chapter 6 summarizes the work and gives a brief personal summary.

## 2 Radio Frequency Identification (RFID)

RFID is a technology based on radio signals that is used all over the world with the main purpose to identify and to track objects. Wherever a need exists for verifying, tracking, or authenticating RFID can help to improve the process. Its ability to communicate over wide ranges without having a need to know the exact position of the tracked objects makes it excellent for supply chain management and in logistics. RFID can be used to answer different types of questions regarding an object:

- Object identification => **Who are you?**
- Object tracking => **Where are you?**
- Object investigation => **How are you?**

Since the most aspects in RFID are very similar to NFC the following chapter gives a detailed overview regarding this contactless technology, its components, the way they act together and possible applications.

### 2.1 RFID-History

The roots of the RFID technology can be found in World War 2. Trying to handle the problem of friend and foe identification the Germans discovered, that rolling the airplane when returning to the base results in a change of the reflected radio signal. As a result the first passive RFID system was discovered. In the same war Watson Watt, who has also invented the predecessor of RFID, the radar, developed the first active RFID for the British airplanes. A transmitter attached to an airplane was used to react on a received signal from a radar station. The main problem of the radar was solved, namely that it was able to identify an aircraft but not to tell if the airplane was a friend or a foe. In the 1950s experimentation with RFID continued. During this time the first electronic anti-theft system was developed. A transponder which saves only 1-Bit gives the information whether a product has been paid or not. Such tags are still used today. (Violino, The History of RFID Technology, 2005)

The concept used then is almost the same nowadays. Readers can communicate with tags, attached to any objects, in a wireless way.

In the 1970ies the first patent for an active RFID tag with rewritable memory was issued. Also a passive RFID transponder was developed, which was used to unlock a door. (Tamm & Tribowski, 2010)

In the 1980ies the technology was made available to the population. The main RFID fields of application can be found in animal tracking, keyless entry, anti-theft- and toll systems. (Hunt, Puglia, & Puglia, 2007)

In 1999 the Auto-ID Center was founded at the Massachusetts Institute of Technology (MIT). The main idea was to enable IT-Systems to identify everyday objects with the help of RFID. This was the birth of the Electronic Product Code. To

keep the costs of the RFID tags low only a serial number was put on a tag. A database that is accessible over the Internet holds the information to this serial number. This invention was a milestone in the use of RFID. (Violino, The History of RFID Technology, 2005)

## 2.2 Auto-ID Center

This organization was set up 1999 with the goal to develop an Electronic Product Code with the purpose to identify and track products through their supply chain. It is unlikely that a tag on a product, which is sent to a manufacturer, will ever return to the supplier again for reuse. Because of this, the main focus was set to the development of low-cost systems. Another requirement for such systems refers to their read range. Companies need the ability to read tags from distances of up to 3 meters. To ensure this read range, the tags need to work in the ultra-high frequency (UHF) band. (Violino, What is RFID, 2015)

In order to track products through their supply chain, around the world, it has to be considered, that such a system has the need to be globally available. Another important issue about a system that has to work for companies in different parts of the world is the interface protocol that is used. Standardization is needed, which in fact should ensure the demand of being freely available to manufactures and end-users. (Violino, What is RFID, 2015)

To access the information of a serial number, which is stored on a tag, a network architecture – integrated in the Internet – was introduced. For reasons of cost and effectiveness special attention was paid to standardization. (Violino, What is RFID, 2015)

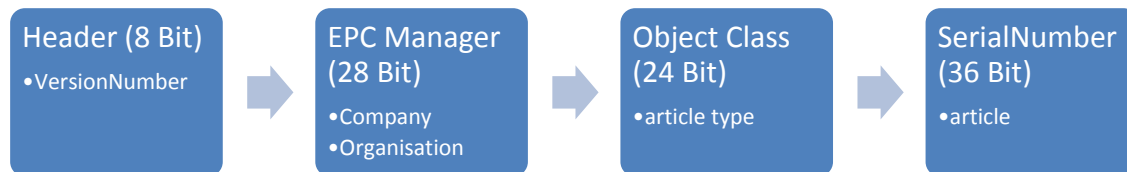
These aspect results in the following key requirements:

- Ultra-high frequency band for read range of up to 3.3 meters
- Low cost – need of disposable tags
- Identify products through supply chain
- Globally available and use of open standards
- Network architecture for accessing information easily available and low cost

### 2.2.1 Electronic Product Code (EPS)

The Electronic Product Code was one outcome of the researches made by the Auto-ID Center. The EPC can be seen as an improvement of the standard Barcode. The idea is to get a big database of identification codes in which each object has its own unambiguous ID forever and always. This ID is saved on an RFID tag and attached to the object it identifies. Today the EPC-standard is only used for passive RFID tags working with UHF. The goal is to get information regarding the condition of an object,

where it is, what is happening with, etc. The great advantage of EPC compared to the standard Barcode is, that RFID tags can be read much faster and over longer distances (up to 10 meters) which make them valuable in supply chain management. Since 2003, EPCglobal Inc. maintains the EPC standard. EPCglobal Inc. is a non-profit organization with the goal to develop standards regarding the format and the way of saving information on tags. The organization has introduced the EPCglobal-Network. This technology allows trading partners all over the world to access and exchange real time data to an EPC-product over the Internet. The recommended structure of an Electronic Product Code is shown in Figure 1. (Ahson & Ilyas, 2008)



*Figure 1: EPC Global structure 96-bit version (Kern, Anwendung von RFID-Systemen, 2006)*

The advantages are obvious:

- Long read ranges (up to 10 meters)
- Passive tags are cheaper and require less maintenance than active tags
- Good read rate (up to 30 Kbit/s)
- Multiple tags can be read at “a time”



## 2.3 RFID-Infrastructure

A RFID-system consists of (Tamm & Tribowski, 2010):

- A transponder, which is attached to the object that should be identified (like a Barcode).
- A reader, which is capable of reading from (and writing to) the transponder.

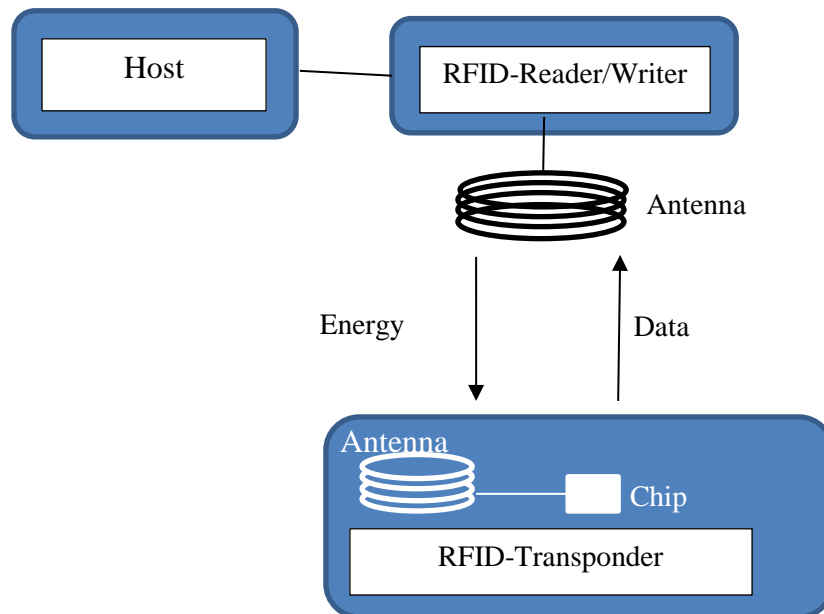
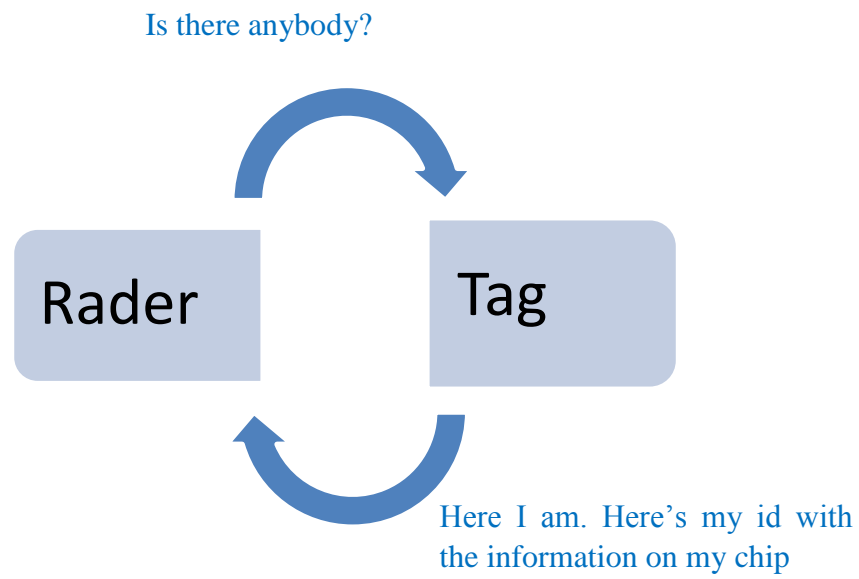


Figure 2: RFID components (Tamm & Tribowski, 2010)

Figure 2 gives a short summary of the main participants in an RFID system. The transponder consists of a microchip and an antenna. The reader is composed of a radio frequency transceiver, an antenna, and a control unit. The communication between reader and tag is simple as depicted in Figure 3. The reader is looking for tags in its field. A transponder gets activated when it is in range of the reader. The transponder receives the required energy for the activation contactless through the coupling unit. As a response the transmitter sends its content to the reader. (Tamm & Tribowski, 2010) (Finkenzeller & Müller, 2010)



*Figure 3: communication Reader and Tag*

## 2.3.1 RFID-Transponder

Transponders, also known as RFID tags, come in different forms like labels, boxes or plastic cards. To identify an object a tag is attached to it. Figure 4 shows the basic components of a tag. It consists of an antenna and a chip. The chip contains product-specific information, whereas the antennas purpose is to respond to an incoming signal from the RFID reader. The housing is depending on the application and can differ from tag to tag. (Castro & Wamba, 2007) (Aguirre, 2007)

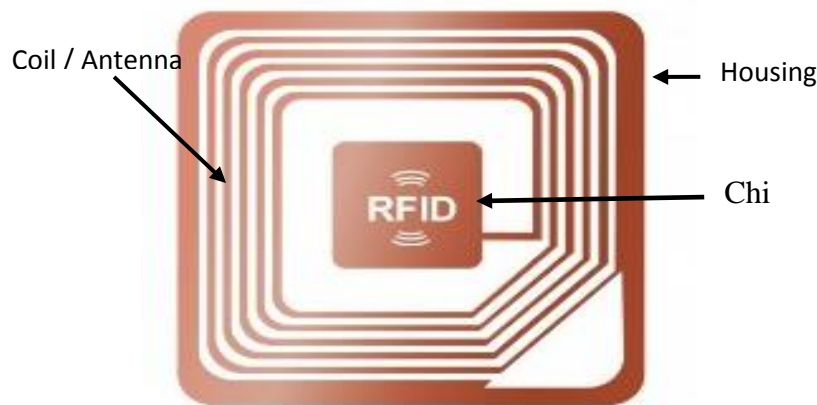


Figure 4: RFID Transponder<sup>1</sup>

Depending on different criteria, transponders can be divided in six main categories. The most important criteria regarding tags are (Castro & Wamba, 2007):

- read range
- capacity of their data storage
- memory type
- energy supply
- size
- the cost

---

<sup>1</sup> [http://www.csols.com/wordpress/wp-content/uploads/2012/12/14757828\\_s.jpg](http://www.csols.com/wordpress/wp-content/uploads/2012/12/14757828_s.jpg)

### 2.3.1.1 Transponder Classes

To get a better overview of the different types of tags EPCglobal has defined six classes for RFID-transponders as depicted in Figure 5. (Tamm & Tribowski, 2010)

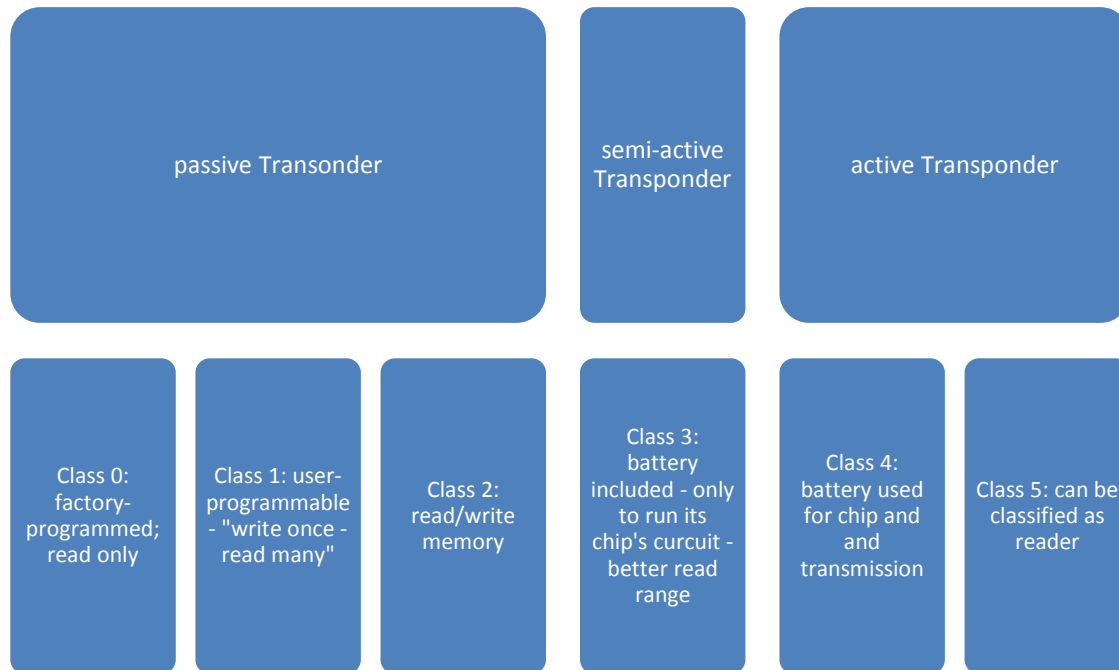


Figure 5: Transponder Classes (Tamm & Tribowski, 2010)

Transponders can be divided into two main categories:

- passive tags and
- active tags

#### 2.3.1.1.1 Passive Transponder

Passive tags are powered by the electromagnetic energy, which is transmitted by a reader. After the transponder gets powered, it starts transmitting the information that is stored on it. These types of transponders are cheaper than active tags. Because of the lacking battery they are also smaller and thinner, which makes them, together with their low costs, a very attractive technology for business. Passive tags have a reading range from 3 centimeters to 10 meter depending on the used frequency. (Want, 2006) (Aguirre, 2007)

### 2.3.1.1.2 Active Transponder

This type of tag needs its own power source to broadcast a signal. It is capable of actively starting the communication and sending information. Active tags only communicate if a reader is in their range; otherwise they go to “sleep”. The read range of active tags (up to 30 meter or more) is much longer, compared to passive transponders. (Want, 2006) (Aguirre, 2007)

### 2.3.1.1.3 Semi-active Transponder

Semi-active tags are a mixed form of active and passive tags. A semi-active tag has its own battery, which is used to drive the operating power. For transmitting information only the power of the reader is used. Their reading range can be up to 30 meter like the range of active tags. (Aguirre, 2007)

## 2.3.1.2 Construction Formats

Transponders can be found in many different design formats. Which design is the best for a transponder, depends on its purpose (Finkenzeller & Müller, 2010):

- Glass Housing: One very promising field of use for RFID is animal tracking. For these purpose small glass transponders (12-32 mm) can be injected under the skin of animals (Figure 7).
- Plastic Housing: Transponders with a plastic housing have been developed for high mechanical demands. The tags can be integrated into car keys or key chains for example (**Error! Reference source not found.**).
- Clocks: This format is often used for access control systems (e.g. ski passes).
- Smart Cards: this format is increasingly rising in the last years, especially in the payment sector (**Error! Reference source not found.**).
- Smart Label: Paper-thin tags are very flexible, which makes them perfect for goods of all types. This format type is a good alternative to Barcodes (Figure 9).



Figure 6: A key chain is a very popular example of a RFID-tag with a plastic housing. This type of tags typically comes with a larger memory.<sup>2</sup>



Figure 8: RFID smart cards are typically used for access control and the payment sector.<sup>4</sup>

Figure 7: LF glass tags are available in different sizes (12-32 mm). The main use case is the identification of animals.<sup>3</sup>



Figure 9: RFID smart label can be found in many forms and sizes. This type of tag is very popular as an alternative to QR Codes and Barcodes.<sup>5</sup>

---

<sup>2</sup> <http://hub360.com.ng/wp-content/uploads/2015/01/rfid-tag-keychain.jpg>

<sup>3</sup> <https://www.rfidcanada.com/wp-content/uploads/2012/09/Glass-tag3.jpg>

<sup>4</sup> [http://www.spartansofttech.com/images/smart\\_card.png](http://www.spartansofttech.com/images/smart_card.png)

<sup>5</sup> <http://www.unipress.de/wp-content/uploads/2014/img/rfid.jpg>

### 2.3.1.3 Frequency, Range and Coupling

The behavior of a tag in terms of its read-range, its costs, and its permeability regarding different materials depends on the used frequency. RFID tags can be distinguished into 3 different kinds of frequency ranges. The following chapter gives a brief overview of the different frequency ranges and their meanings.

#### 2.3.1.3.1 Frequency

Each frequency results in a different radio waves behaving as can be seen in Figure 10. The behavior of electromagnetic waves tends to be increasingly similar to light the higher the frequency becomes. For this reason there may be stronger reflections, the higher the frequency gets. Waves operating at low frequency can permeate water, whereas higher frequencies are losing this ability, instead the energy is converted into heat. Because of this, transponders working with UHF are not usable for objects containing water, animals, or people. Depending on the purpose of the application, different frequencies are recommended. Active tags typically operate at the Ultra High Frequency band (455 MHz, 2.45 GHz or 5.8 GHz). Passive tags can operate at low frequency, high frequency, and ultra-high frequency. (Violino, The basics of RFID technology, 2005) (Kern, Anwendung von RFID-Systemen, 2007)

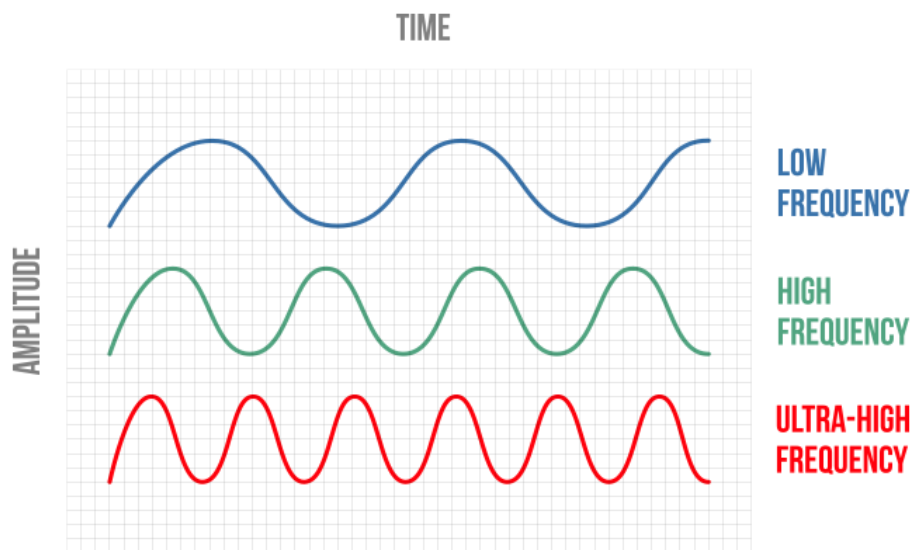


Figure 10: Amplitude change based on frequency<sup>6</sup>

<sup>6</sup> <http://containertracking.how/Technology/RFID>

#### *2.3.1.3.1.1 Low-frequency (125 kHz, 135 kHz)*

Radio transmission works in the field of low-frequency. The waves in this frequency spectrum can travel through walls, but they are insensitive to metal or liquid. Because of these capabilities this kind of transmission is mostly used for identification of objects with high water content. Applications working at low-frequency have a read range of up to 50cm. (Tamm & Tribowski, 2010) (Violino, RFID Journal, 2005)

Good for: Animal-tracking, access control, immobilizer

- Short read range
- Read speed slower than higher frequencies
- Good for reading at close range as well as for metal and water surfaces
- Frequencies from 30kHz to 300kHz possible

(Tamm & Tribowski, 2010)

#### *2.3.1.3.1.2 High-frequency (6.78 MHz, 13.56 MHz, 27.125 MHz and 40.680 MHz)*

Compared to low-frequency tags, this type of tags result in much faster data transfer, higher read ranges (up to 100 cm), and a greater absorption of power. Even though frequencies between 3 MHz and 30 MHz are possible. The typical frequency rate used is 13.56 MHz. (RFIDJournal, RFID Journal)

Good for: ticketing, contactless payment systems, access control

HF tags can store up to 8 kilobytes of data, which should be considered if the amount of storage area is important. UHF for example can only store between 24 and 110 bytes of data. (Tamm & Tribowski, 2010)

#### *2.3.1.3.1.3 Ultra-High-frequency: 860 MHz – 960 MHz*

These systems can have a read range of up to 12m at very fast transfer rate. This frequency spectrum is much more sensitive to reflections caused by surfaces than the other two. The big advantage of UHF is that RFID tags operating at this frequency spectrum are much easier and cheaper to manufacture. Because of the read range, its simplicity, and low cost UHF tags are getting most attractive for manufacturers, especially for supply-chain applications. Consequently this standard is the fastest growing segment in the RFID market. (Tamm & Tribowski, 2010) (Violino, RFID Journal, 2005)



### 2.3.1.3.2 Coupling and Read Range

The technology that is used for transmitting data from a tag to a reader is one of the most important factors regarding the read range. Coupling can be distinguished into two categories as illustrated in Figure 11.

#### Inductive coupling

- close coupling
- LF and HF

#### Electromagnetic backscatter

- remote to long-range coupling
- UHF

Figure 11: coupling types in RFID

#### 2.3.1.3.2.1 Inductive coupling

Inductive coupling works with a magnetic field to transmit data from the reader to the tag. This coupling method is mostly used for low- and high-frequency tags operating in passive mode. Inductive coupled systems use coils for antennas. The reader produces a HF electromagnetic field. When the tag is placed close enough to enter this field, the coil of the reader and the coil of the tag form a wireless energy coupling. The simplest form of such a coupling is described by a transformer. A transformer consists of a unit with a primary and a secondary coil (Figure 12). The current change in one coil results in a flux change in both coils, which in turn lead to a voltage induction in the second coil. (Finkenzeller & Müller, 2010) (Langer & Roland, 2010)

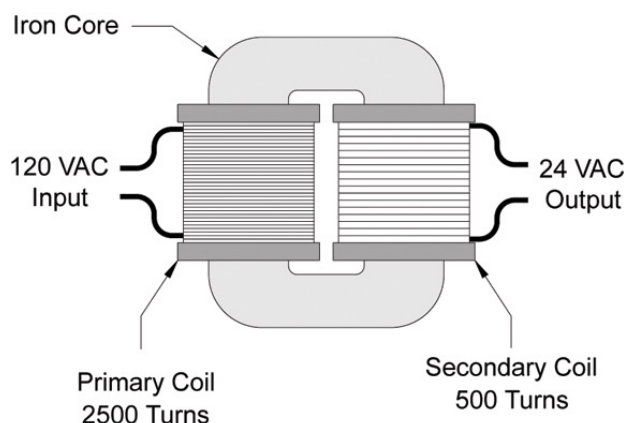


Figure 12: Basic Transformer Components (Elliott, 2009)

Figure 13 describes the basic principle of an inductively coupled RFID system. More, it also explains why it is sufficient if only the reader has an energy source. The

primary coil (reader) has a voltage source. If the two coils (reader and tag) get together they form a magnetic field, allowing the reader to induce voltage into the second coil.

The voltage that is induced into the second coil depends on the number of turns of the coil, its size, and the frequency of operation. (Dobkin, 2008)

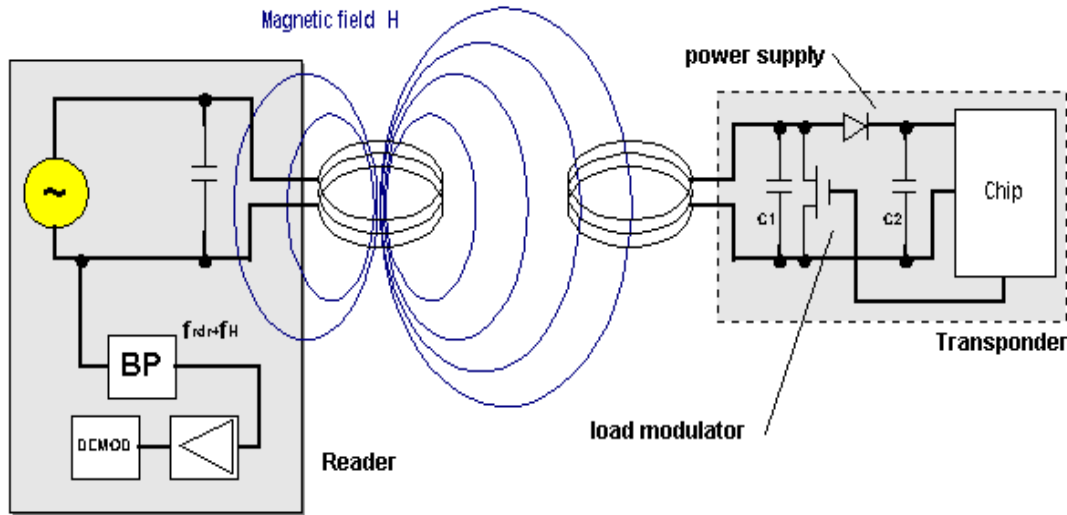


Figure 13: Inductive coupled RFID system (Finkenzeller & Müller, 2010)

The disadvantage of this method is obvious. The magnetic field gets weaker the farther away the tag. If the tag leaves the range of the magnetic field, the coupling between the coils gets lost, the tag loses its power supply and because of that the transmission is no longer possible. For this reason, these systems are advisable for short range communication. (Finkenzeller & Müller, 2010)

#### 2.3.1.3.2.2 Electromagnetic Backscatter Coupling

This type of coupling is used for long-range communication between reader and transponder, working at UHF (868 MHz Europe, 915 MHz USA) and at microwave frequencies (2.5 GHz Europe, 5.8 GHz USA). (Finkenzeller & Müller, 2010)

The tag that is used for backscatter coupling works in active mode. Because of the long ranges the transponder does not get enough energy from the reader to power its microchip. Hence the microchip needs its own power supply, usually in the form of a battery. This battery is only used to power the microchip. The data-transmission between tag and reader itself works only based on the electromagnetic wave emitted by the reader. A “power down” mode on the microchip is used to prevent the battery from being discharged unnecessarily. If the tag is out of the readers range, this mode is turned on in order to keep the energy consumption as low as possible. (Finkenzeller & Müller, 2010)

In contrast to capacitive coupling, which is using a HF electrical field and inductive coupling, which is using a HF magnetic field, UHF-backscatter systems are working with electromagnetic waves, based on the principle of energy-reflection. (Langer & Roland, 2010)

This method is based on radar technology described in (Finkenzeller & Müller, 2010):

- An object reflects electromagnetic waves, if the dimension of the object is greater than half the wavelength
- The “reflection cross-section” describes the power of a reflected wave.
- If the object is in resonance with the incoming wave (e.g. antennas operating at the same frequency) the reflection cross-section is particularly large.

Figure 14 shows how the communication works (Finkenzeller & Müller, 2010):

- The reader emits a power  $P_1$
- A part of this Power ( $P_1'$ ) arrives at the tag
- A rectifier (diodes  $D_1$  and  $D_2$ ) is used to convert the alternating current to direct current
- The resulting voltage is used for activation/deactivation of the “power down” mode
- One part of the incoming power is reflected by the tag ( $P_2$ ) – this energy is scattered back to the receiver input of the reader

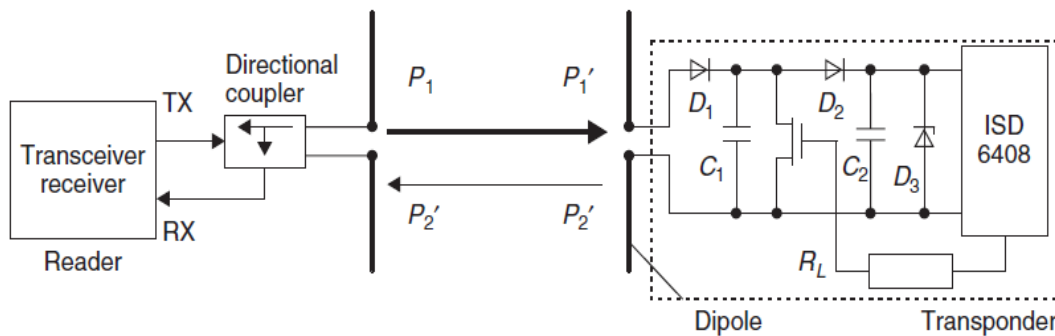


Figure 14: Electromagnetic Backscatter coupling (Finkenzeller & Müller, 2010)

In Table 1 the different frequency ranges used by transponders are summarized in order to get a better overview.

## 2.3.1.4 Transponder Overview

	LF	HF	UHF	SHF
<b>Frequency</b>	125 kHz	13.56 MHz	858-930 MHz	2.45 GHz – 5.8 GHz
<b>Physical coupling</b>	Inductive coupling	Inductive coupling	Electromagnetic field	Electromagnetic field
<b>Max. Read Range</b>	30cm – 1 m	10cm – 1 m	Passive: <=25m Active <=100m	Passive:<=1m Active: <= 50m
<b>Reading Speed</b>	Up to < 1 Kbit/s	Up to 25 Kbit/s	Up to 30 Kbit/s	Up to 100 Kbit/s
<b>Antenna size</b>	Largest	Large	Small	Smallest
<b>Permeability</b>	<ul style="list-style-type: none"> <li>✓ Plastic</li> <li>✓ Oils</li> <li>✓ Liquids</li> <li>✓ Some metals</li> <li>- Dense materials (brick, metals...)</li> </ul>	<ul style="list-style-type: none"> <li>✓ Oils</li> <li>✓ Paper</li> <li>✓ Dry wood</li> <li>✓ Most plastics</li> <li>- Dense materials</li> <li>- Wet wood</li> <li>- Snow</li> </ul>	<ul style="list-style-type: none"> <li>✓ Oils</li> <li>✓ Paper</li> <li>✓ Most plastics</li> <li>- Dense materials</li> <li>- Liquids</li> </ul>	
<b>Applications</b>	<ul style="list-style-type: none"> <li>• Animal tracking</li> <li>• Access control</li> </ul>	<ul style="list-style-type: none"> <li>• Ticketing</li> <li>• Contactless payment</li> <li>• Access control</li> <li>• Security requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Pallet tracking</li> <li>• Industrial automation</li> <li>• Asset management</li> <li>• Access control for vehicles</li> <li>• Inventory management</li> </ul>	<ul style="list-style-type: none"> <li>• Real time location of goods</li> <li>• Highway toll tags</li> <li>• Asset management</li> </ul>
<b>Standards</b>	<ul style="list-style-type: none"> <li>• ISO 11784</li> <li>• ISO 11785</li> <li>• ISO 14224</li> </ul>	<ul style="list-style-type: none"> <li>• ISO 14443</li> <li>• ISO 15693</li> <li>• ISO 18000-3</li> </ul>	<ul style="list-style-type: none"> <li>• ISO 18000-6</li> <li>• EPC Gen2</li> </ul>	<ul style="list-style-type: none"> <li>• ISO 18000-4</li> <li>• IEEE 802.11</li> <li>• IEEE 802.15.4</li> </ul>

Table 1: RFID frequency overview (Violino, What is RFID, 2015) (Corporation, 2007) (Ferrer, Dew, &amp; Apte, 2010)

## 2.3.2 Communication Mode

This passage focuses on the way readers and tags communicate. The data transfer from the reader to the transponder is referred to as down-link. The transfer from the tag to the reader is called up-link. The communication can be distinguished in three different kinds as depicted in Figure 15 (Finkenzeller & Müller, 2010) (Glover & Bhatt, 2006):

- Full-duplex (FDX)
  - Reader and tag talk at the same time
  - Down-link and up-link can overlap
  - Uses mostly separate frequency bands for sending and receiving
- Half-duplex (HDX)
  - Reader and tag alternate in communication
  - No overlapping between down-link and up-link possible
  - The transmitter is switched off when a signal should be received
- Sequential (SEQ)
  - Reader and transponder have only a limited period of time for their communication before they switch
  - Down-link during the energy transfer from the reader to the transponder
  - Up-link in the pause of the energy transfer

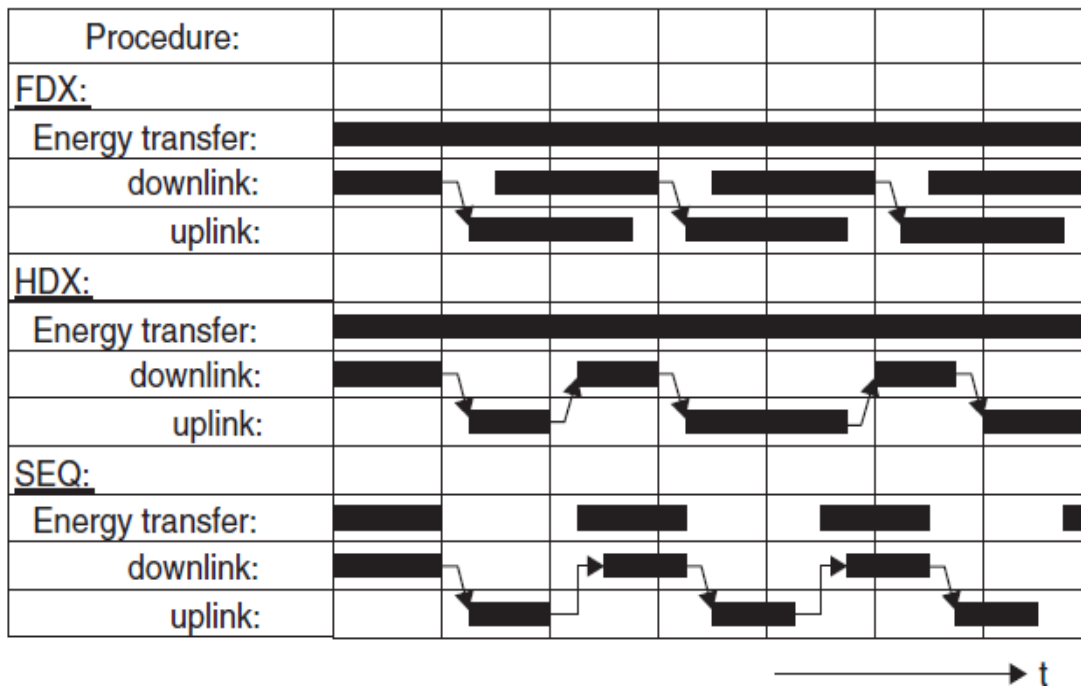


Figure 15: RFID communication mode (Finkenzeller & Müller, 2010)

### 2.3.3 RFID Reader

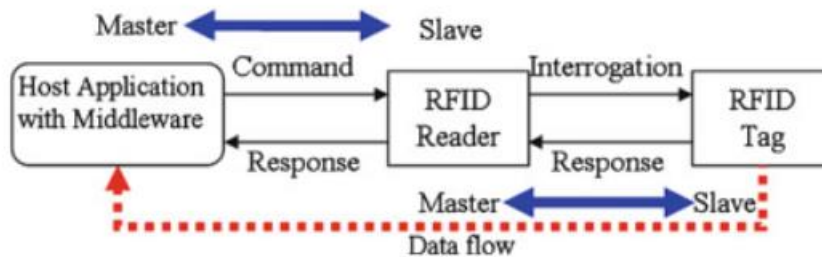


Figure 16: Master-slave principle RFID participants (Preradovic & Karmakar, 2012)

The concept of an RFID reader is shown in Figure 16. The reader acts as interrogator for the tags. Once the reader detects a transponder it starts extracting data from it. Reader and transponder have a master-slave relationship to each other, which means, based on techniques in the previous chapter (induction, electromagnetic waves) the reader activates the tag. After that the transponder starts generating signals and sending them back to the reader. The reader in turn is a slave to the middleware, a software application that sends commands to the reader. (Preradovic & Karmakar, 2012)

RFID systems have to face a lot of requirements. An ideal RFID system would have to fulfill different needs. The following example shows the problems that could possibly occur in respect to those needs.

As described in (Preradovic & Karmakar, 2012) an ideal RFID system would have to satisfy the following conditions:

- An exact read range, meaning tags in the range of the reader can be recognized with 100% accuracy, whereas tags outside the read range are not affecting the reader in any way, meaning the read rate for such tags is 0%,
- The physical orientation of the tag, its environment and the composition of the object it is placed on has no effect on the performance of the system.
- The communication between one reader and multiple tags works without any collision. N outgoing requests from the reader result in N incoming answers from the addressed transponders.
- Multiple tags and multiple readers are not affecting the performance of the system.
- The system is in-vulnerable to security issues
- The cost for creating the RFID system is low.
- The integration of the RFID software into existing software, as well as the synchronization between multiple readers is simple and cheap.

These requirements demonstrate that such a system cannot exist. More important, they show which problems have to be thought of.

### *2.3.3.1 Components*

Even though many different types of RFID readers exist, all of them have three major components in common (Karmakar, Koswatta, Kalansuriya, & E-Azim, 2013):

- Antenna
  - Transmit and receive signals
  - A reader can have multiple antennas for different circumstances (e.g. one antenna for receiving and another antenna for transmitting data)
- Radio-frequency (RF) section
  - Contains two signal paths for the transmitter and the receiver circuits
  - Generates the power which activates a transponder
  - Creates the signal for sending data to the transponder
  - Extracts the signal response from the tag
- Digital control section
  - Consists normally of a microprocessor, analog to digital converters and a memory block
  - Controls the RF section

### *2.3.3.2 Types of readers*

The reader can be classified base on different criteria. An overview of the most important criteria is shown in Figure 17.

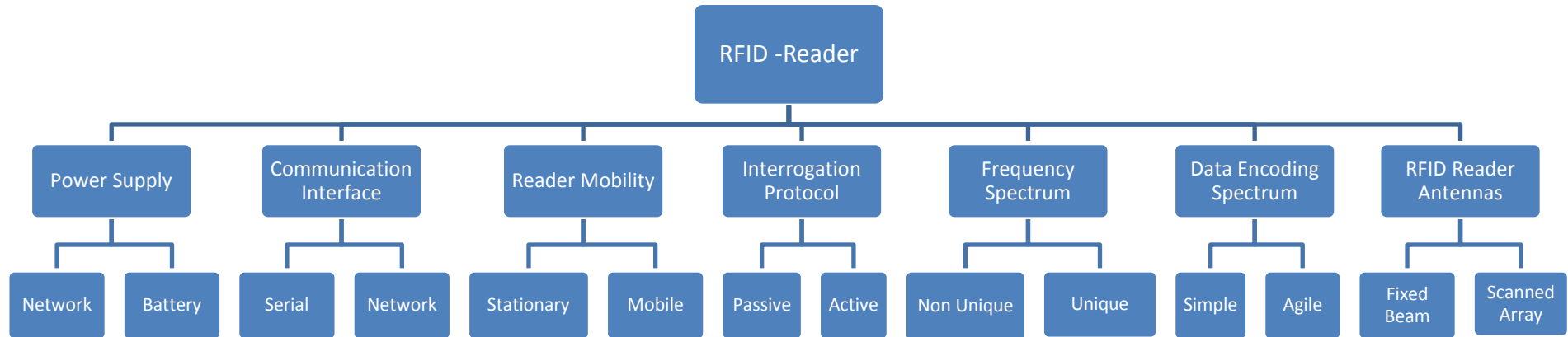


Figure 17: types of available RFID readers (Preradovic & Karmakar, 2012)



2.3.3.2.1 Classification regarding power (Karmakar, Handbook of Smart Antennas for RFID Systems, 2011):

- Supplied from a power network
  - Mostly used for stationary readers
  - Operation voltage from 5 to 12 V
- Supplied by a battery
  - Good for portable readers
  - Battery powers the motherboard of the reader
  - 5 – 12 V

2.3.3.2.2 Classification regarding communication interface (Karmakar, Handbook of Smart Antennas for RFID Systems, 2011)

- Serial readers
  - Communication with host computer happens over a serial communication link
- Network readers
  - Communication with host computer happens over a wired/wireless network
  - Supports multiple protocols (TCP/IP, UDP/IP, HTTP) and standards (Ethernet (IEEE-802.3), Wi-Fi (IEEE 802.11))

2.3.3.2.3 Classification regarding the mobility (Karmakar, Handbook of Smart Antennas for RFID Systems, 2011)

- Stationary readers
  - Permanent location, for example attached to walls, doors, etc.
- Mobile readers
  - Can change their position, as they are attached to moving objects or can be carried by human.

#### 2.3.3.2.4 Classification regarding the interrogation protocol (Karmakar, Handbook of Smart Antennas for RFID Systems, 2011)

- Passive readers
  - Only listening
  - The only signal the reader sends is a power signal to activate the transponder, after which it starts listening for the tags unique ID
  - 1-Bit-transponder
- Active readers
  - Interrogation and listening
  - The reader activates the tag, interrogates signals and receives replies from the tag

#### 2.3.3.2.5 Classification regarding the frequency spectrum (Karmakar, Handbook of Smart Antennas for RFID Systems, 2011)

- Unique frequency-response-based readers
  - This type of reader operates at a single frequency range (< 80 MHz)
  - The same frequency is used for sending and receiving
  - Mostly commonly used
- Non-unique frequency-response-based readers
  - Two frequency bands are used
  - One frequency is used for sending commands
  - The other frequency is used for receiving answers
  - Fast and reliable
  - Used for full-duplex communication
  - Complicated RF front end

#### 2.3.3.2.6 Classification regarding the data encoding protocol (Karmakar, Handbook of Smart Antennas for RFID Systems, 2011)

- Single
  - One protocol is used for communication (sending and receiving).
  - The reader can only communicate with a tag that uses the same protocol.
- Agile
  - This type of reader can handle tags with multiple protocols.
  - Most commonly used

#### 2.3.3.2.7 Classification regarding the antenna (Karmakar, Handbook of Smart Antennas for RFID Systems, 2011)

- Fixed-beam
  - Easy to install

- Tries to cover as much area as possible which can lead to errors because of signals from other sources than the transponder.
- Scanned-array
  - Smart antenna systems used
  - Reduces errors coming from wrong signals

## 2.4 RFID Anti-Collision

Thinking of the communication between a reader and a tag does not sound complicated if you have a rough understanding of the communication process. But how can a reader detect multiple tags in its range (depicted in Figure 18) and even more, how can a reader distinguish the tags during the coupling?

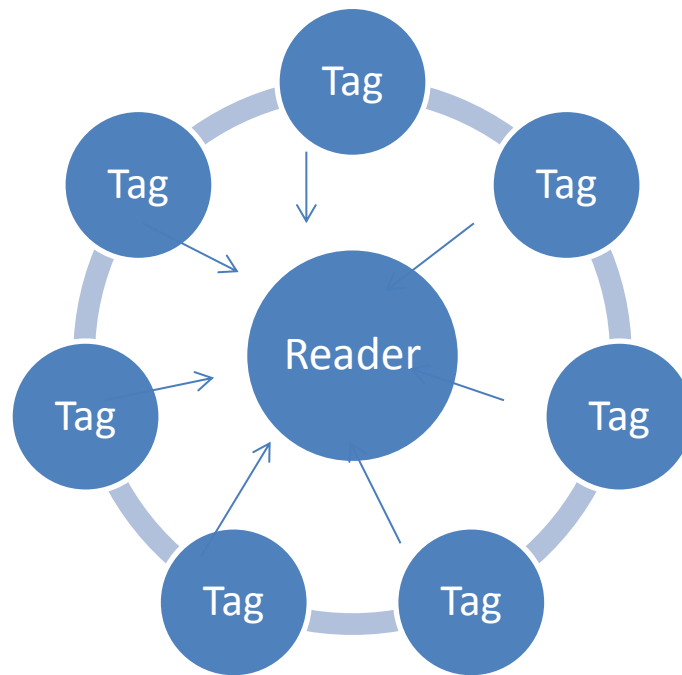
Anti-collision algorithms are a very important element regarding RFID communication between multiple components.

One important thing about anti-collision and multi-access strategies is that we cannot think about multi access just in the way that a reader can read from multiple tags at the same time. The reader has also to recognize which transponder is the right one in a specific situation. One example that illustrates how important multi access strategies are would be a reader that is reading from a Smart Card. If a person has multiple Smart Cards in his/her pocket, which normally is the case, a reader should be able to recognize the correct card even though the whole pocket with all its transponders is in the read range. (Langer & Roland, 2010)

Collisions can be split up into two different types (Shu-qin, Wu-chen, Li-gang, & Wang, 2010):

- Interrogator collisions
  - Happens if multiple readers detect and interrogate a tag at the same time.
- Tag collisions
  - Happens if a reader detects multiple tags at the same time and tries to interrogate them over the same channel simultaneously. In such a case all tags are transmitting their data at the same time. The reader cannot receive them in a correct way.

Depending on the type of tag an anti-collision method can already be provided on the tag itself. An active tag may have the ability to detect other tags in its range because of its on-board battery. Passive tags however have no ability for collision detection. Since passive tags have a wide field of use there is a great need for an anti-collision protocol on the side of the reader, like for example in the supply-chain management, where the probability that more than one tag will be in the range of a reader is very high. (Shu-qin, Wu-chen, Li-gang, & Wang, 2010) (Klair, Chin, & Raad, 2010);



*Figure 18: RFID reader with multiple tags in its read range, all tags try to transfer data to the reader at once*

## 2.4.1 Anti-collision protocols

Today there are different anti-collision protocols in use. Basically we can differ between four main strategies regarding the classification of the subscribers. The strategies are summarized in Figure 19.

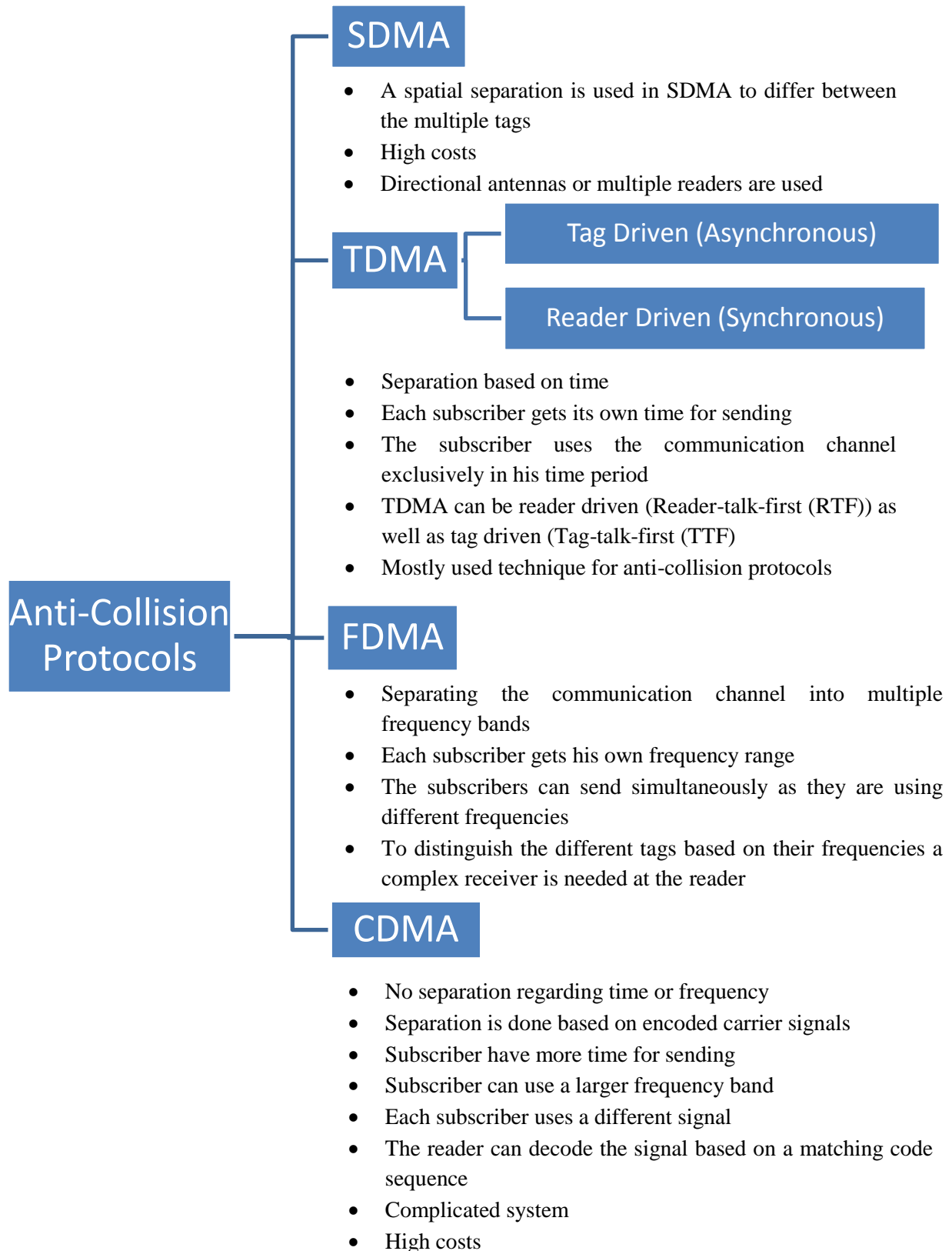


Figure 19: Anti-collision protocols overview (Klair, Chin, & Raad, 2010) (Langer & Roland, 2010)

### 2.4.1.1 *Time Division Multiple Access (TDMA)*

Since most RFID systems use TDMA techniques, we will take a deeper look into its functionality. As you can see in the overview of the anti-collision protocols TDMA is the only one that can be further distinguished into “Tag Driven” and “Reader Driven” protocols.

“Tag Driven” protocols work asynchronously. The data transfer is controlled by the transponders themselves. “Reader-Driven” procedures are the ones most commonly used for collision detection and prevention. Here the reader has the control over the data flow, which makes it possible that this procedure works synchronously. (Shu-qin, Wu-chen, Li-gang, & Wang, 2010)

The advantage of TDMA is that only the time interval of a tag response is taken into account for recognition, which in fact means, that no other restrictions exist (e.g. no restriction regarding the used frequency). (Langer & Roland, 2010)

TDMA can be divided into two categories based on the protocol it uses for collision detection and prevention (Langer & Roland, 2010) :

- Tree-based protocol (Binary search)
- ALOHA-based protocol

### 2.4.1.2 *Tree based protocol*

This type of schema can be referred to as deterministic schema. The most popular representative of this type is the Binary search. (Liu, 2016)

This technique is used for reader driven procedures. The reader uses it to recognize all available tags in its range. Each tag has a unique ID. The reader performs the collision detection based on that ID and a checksum as described in (Langer & Roland, 2010):

- 1) The reader requests the IDs of the tags in its range.
- 2) The tags answer with their ID and a checksum of the request.
- 3) If the reader detects only one transponder the initialization for this tag is finished. The reader can now communicate with it.
- 4) If multiple tags are present a collision will be detected. To reduce the amount of requested tags the reader splits the tags in two groups. Now the request is sent again but only to one of the groups. Only the tags with an ID less or equal to a specific value are allowed to answer.
- 5) Back to 2)
- 6) If no tags can be detected a request is sent to the other group. Go to 2)

A visual example of this schema can be seen in Figure 20.

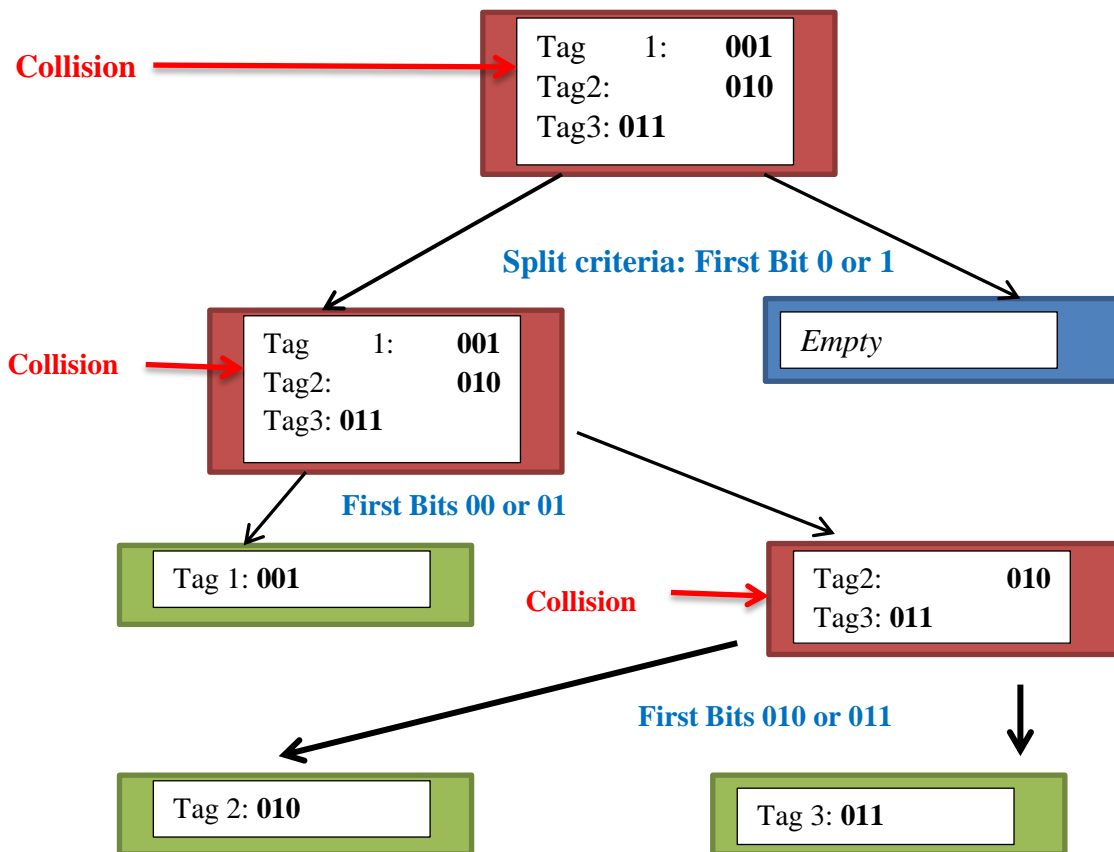


Figure 20: Tree based anti-collision strategy (Shu-qin, Wu-chen, Li-gang, & Wang, 2010)

### 2.4.1.3 ALOHA based schema

The ALOHA procedure is working with a transponder-driven mechanism. This kind of anti-collision technique is based on probability. The transponders choose their timeslot for sending randomly. If a collision occurs the sending is repeated. This procedure is very slow compared to reader-driven procedures.

*Slotted ALOHA* is an enhancement to the conventional version. Here the reader again requests the IDs of the transponders. In addition he also sends the transponders information regarding the possible time slots. The tags choose a time slot randomly and answer with their ID. If the reader can recognize a transponder uniquely it deactivates this transponder and sends the request again to the other transponders till all tags in its range are recognized. The request is repeated if a collision is detected. This schema can be faster than the binary search but it gives no guarantee that all tags will be recognized in finite time. (Langer & Roland, 2010)



## 2.5 How many tags can be read?

Reading one tag after another can be very fast. Aside from the collision problem, reading multiple tags can be a problem if they are not long enough in the readers range. Thanks to the anti-collision technologies, a reader can now identify multiple tags. The identification process happens of course not for all tags at once, but due to the high speed at which the reader identifies a single tag, identifying many tags in range happens almost simultaneously. (RFIDJournal, RFID Journal) To get a rough idea, a reader can communicate with up to 50 tags one after another within milliseconds (RFIDJournal, RFID Journal, 2013). This gives the impression that it happened at the same time.

How many tags can be identified by a reader and how long the identification process takes depends on the kind of tag that is used. As it has been mentioned already we can differ between active and passive tags with frequencies starting at 127 kHz up to 5,6GHz. Depending on the tag type that is used and the frequency it operates on the read range and speed will differ. Transmitting data from a tag operating at low frequency (127 kHz) for example will take more time than transmitting data from a tag operating at high frequency (13.35 MHz).

Beside the frequency of the tag the amount of time that it spends in the area of the reader is very important. Identifying multiple tags if they are for example moving through a door will not work correctly. The reader won't be able to identify all tags. Having readers on all four sides of a tunnel (2 readers at start of the tunnel and 2 readers at the end) and moving the same tags through this tunnel on the other site will result in the identification of all tags in a few seconds. Another problem that can occur is that the tags are blocking the signal of each other if they are too close. If the tag in front blocks the signal no energy can reach the tag behind, therefore it cannot be read. The easiest solution to this problem is to keep a certain distance between the transponders. (RFIDJournal, How Many Tags Can Be Read By an RFID Reader at One Time?, 2011) (RFIDJournal, How Can an RFID Reader Interrogate Multiple Tags Simultaneously?, 2010)

## 2.6 Security Requirements

Depending on the field of use, RFID systems need to satisfy different degrees of security requirements. Whereas security has not the first status regarding systems that are used in a closed industry, it is most important when considering applications connected with money.

Like each system that is transferring data the risk of attacks is very present for RFID systems as well. How does the reader know that he is talking to the transponder he expects to talk to? Men in the middle attacks are quiet common for telecommunication systems. How vulnerable is the transponder for manipulation and unauthorized access?

A tag itself probably will not contain sensible data, but it can contain an ID which is the key for object-specific information (e.g. tag location, price, etc.) in a database. A manufacturer probably does not want this information's to be accessed by unauthorized parties

The most attractive characteristic of RFID tags is their price. Low costs allow manufacturers to switch to this technology. The problem with cheapness is that high quality and high quantity usually do not go along. The MIT Auto-ID Center is working permanently on researches projects regarding low-cost RFID tags. But for now, we can assume that cheap and secure tags do not exist.

### 2.6.1 Attacks

An RFID system is vulnerable to attacks to basically each component. Figure 21 gives a good overview of the parts of an RFID system and its weak points.

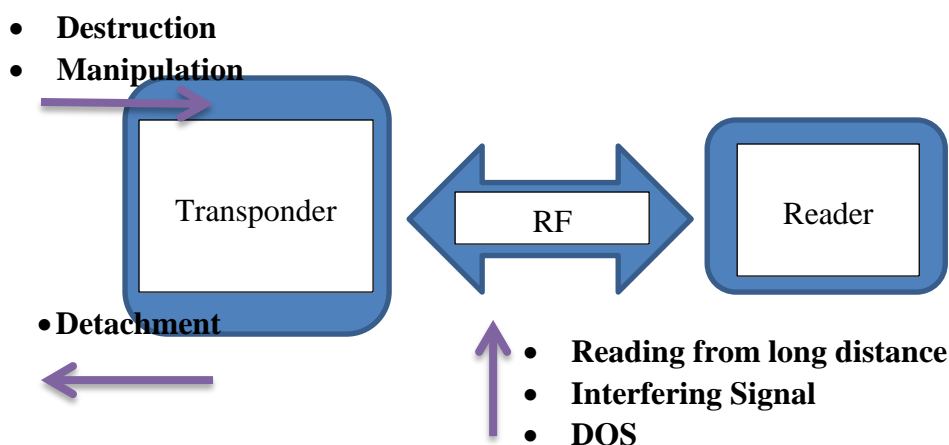


Figure 21: Possible Attacks RFID (Finkenzeller & Müller, 2010)

The following section describes some of the possible attacks depicted in Figure 21.

### 2.6.1.1 *Transponder attacks*

The tag represents the part of a RFID system that is easiest to attack because of its accessibility. Some attacks regarding the transponder may be (Finkenzeller & Müller, 2010):

- Destruction
  - This kind of attack is the most vulnerable to a tag as it is permanent. It refers directly at destroying the tag in a mechanical or chemical way.
  - Putting the transponder into a microwave oven for example would produce higher field strength than the tag can withstand, this would lead to thermal destruction.
  - Further examples can be:
    - Energy attacks
    - Removing of material (e.g. antenna)
    - Crushing the tag
    - Etc.
- Detachment:
  - It is not necessary to destroy a tag to make it unusable. Shielding can prevent a transponder from being identified by a reader.
  - Example: aluminum foil around the tag makes it “invisible” for the reader.
- Manipulation:
  - By reading a tags information an attacker may be able to clone this tag and to start communicating with the reader by himself.
  - Very easy for read-only transponders
  - Read-write tags have often memories that can be accessed without any authentication (i.e. key, password). Manipulating this memories is also a good application point for attackers
  - Read-only tags and tags with unprotected memory have to be avoided for entrance systems

### 2.6.1.2 *RF-Interface attacks*

There is no need to have physical access to a tag to attack an RFID system. An attacker could have the opportunity to misuse such a system from a distance because of the RF-Interface.

- Reading from a long distance
  - An attacker is able to intercept the communication between reader and tag from a distance
  - Studies have shown that it is possible to intercept a RFID communication operating at 13.56MHz from a distance of up to 3 meter. (Finkenzeller & Müller, 2010)
  - Encrypting the transmitted data can be a good protection against such attacks. (Finkenzeller & Müller, 2010)
- DOS
  - The goal is to prevent a tag from receiving data from the reader.
  - The attacker sends the reader a large number of serial numbers. The reader tries to determine the serial number which blocks him totally. The result is that the reader is not able to detect any tag correctly. (Finkenzeller & Müller, 2010)
- Interfering signal
  - This type of attack is also called Jamming.
  - This type of attack temporarily disables the tag (e.g. by using an aluminum foil to shield a tag from electromagnetic waves) (Aikaterini Mitrokotsa)
- Eavesdropping
  - This attack is one of the greatest threats to RFID. The greater the read range of a reader the easier it is to trap the intercept the signal.
  - By using an antenna the communication between reader and tag is captured by an attacker. (Aikaterini Mitrokotsa)

## 2.7 RFID applications

The following RFID applications are just a few examples of how RFID can be used. Beside the standard use cases regarding tracking and controlling, RFID gives great opportunities in areas of advertising, customer acquisition, and marketing. The limits regarding its use are created by your imagination.

### 2.7.1 Supply Chain Management (SCM)

All activities regarding materials, information's, and finances in a company are tracked and coordinated in the supply chain management. Different entities are involved in the chain process. How a manufacturer gets the needed materials for a product? From who are the materials received? How does the final product finally reach the customer? All this are questions a supply chain management has to deal with. (Quirk & Borello, 2005)

The supply chain management can be divided into three main parts according to (Shah, 2009):

- Product flow
  - Deals with the product itself.
- Information flow
- Finances flow

All information's affecting a product in any way are important (e.g. bills, schedules, shipment, etc.) in SCM. RFID can be an important part of SCM regarding the following points (Sarac, Absi, & Dazere-Peres, 2010) (Tajima, 2007):

- Tracking and identifying goods in real-time (position, sending/arriving time) can improve the time efficiency in a company.
- Different actors can receive important information's to a product anytime and from anywhere. In this way the process of information sharing is made much easier.
- The automated tracking and identification of objects can help to improve the inventory management.
- RFID can also improve the order efficiency.

## 2.7.2 Animal Identification

It already has been mentioned that RFID has reached great success in the field of animal tracking. Regarding the attaching process and the material of the tag, we can differ between 4 basic types described in (Finkenzeller & Müller, 2010). A visual example is given in Figure 22.

- **Injectable transponder**
  - This kind of RFID tag is injected under the skin of the animal.
  - It is good for verification process, as the transponder can only be removed by means of surgery.
- **Ear tag**
  - Is used as a replacement of the standard Barcode ear tags.
  - The advantage is that the tags can be read from a distance of up to 1 meter, whereas Barcode tags require a distance of a few centimeters.
  - Barcode tags on the other hand are cheaper.
- **Collar transponder**
  - This kind of tag can easily be replaced, resulting in wrong identification.
  - When it comes to verification aspects they are not useful.
  - Use cases: automation of the feeding process.
- **Bolus**
  - The bolus is an alternative to the injection.
  - It consists of a ceramic capsule with a passive RFID chip in it.
  - It is administered orally and has a
  - Very high probability to stay in the rumen of the animal for a live time.
  - Easier to remove in the slaughterhouse than an injected tag.

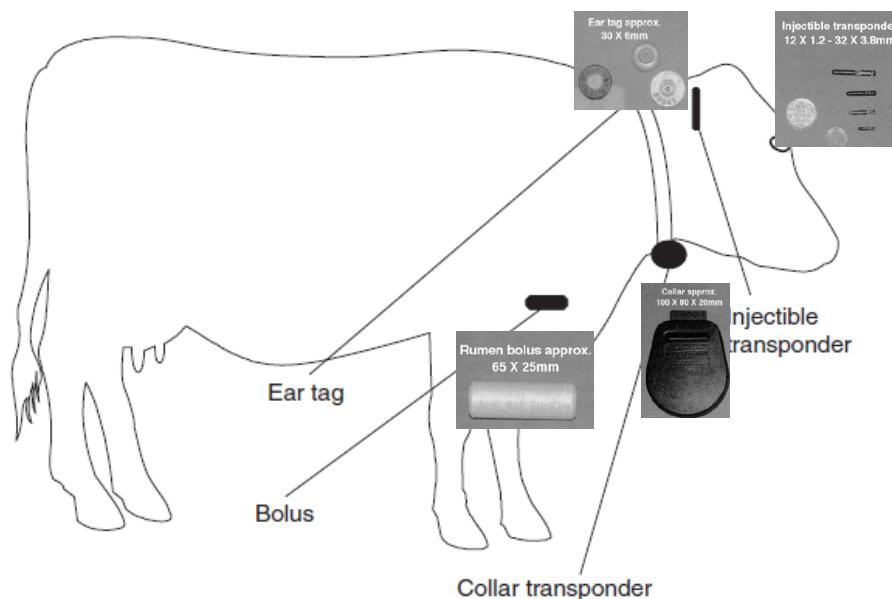


Figure 22: Animal transponder overview (Finkenzeller & Müller, 2010)

### 2.7.3 Budweiser's buddy cup



Figure 23: Buddweiser's buddy cup <sup>7</sup>

A good example of how to make marketing for the own brand in a cheap and funny way is the “Budweiser buddy cup”.

Budweiser Brazil developed cups with an RFID tag and a QR Code on it. The idea is that participant’s sync their Facebook accounts with their glasses over the QR Code. Every time a participant clicks his/her glass with another cup-holder he/she becomes friends with this person on Facebook. (adweek, 2013)

### 2.7.4 Shopping with RFID

Chaotic Moon in Texas is developing a prototype shopping cart using RFID. The idea is that an RFID reader and a tablet are attached to each shopping card. A customer can upload his shopping list to the tablet. Every time he/she adds an item from the list to the cart the item is removed from the list. Furthermore the cart alerts the customer if he/she is adding something to the cart that could cause an allergic reaction. The cart also warns the customer if he/she is adding a wrong item to the card and sums up the final price – making the cash register obsolete. (Thrasher, 2013)

### 2.7.5 Burberrys RFID store

The designer label Burberry attached RFID tags to its clothes in a store in London. Every time a customer enters a fitting room with such an item commercials regarding this particular clothing start playing, giving the customer more information about the design, ideas of combination, etc. (Thrasher, 2013)

---

<sup>7</sup><http://www.adweek.com/adfreak/budweisers-buddy-cup-might-be-dumbest-high-tech-brand-innovation-yet-149048>

## 2.7.6 Electronic Road Pricing System (ERP)

In 1998 the government of Singapore used RFID to create a toll collection system. Tags attached to cars were recognized by readers on the highway. The transaction speed was increased incredible by this system. (Jerry Banks, 2007)



## 2.8 When is RFID the right solution?

RFID has a lot of advantages. Especially in Supply Chain Management where it is important to know where your goods are and when they receive their RFID is a good and usable technology. Even though companies are informing themselves a lot on the topic of RFID and maybe even did small scale studies it is still not as widely used as it would be possible.

One big issue when it comes to changes in companies and their implementation is money. RFID tags are cheap. A unit price of about 0.50 € for a single tag is not worth mentioning. But if you do need 10,000 tags every month this would mean a total of about 5,000 €. RFID is an alternative to Barcodes, paper, and manual tracking. If a company already uses one of these alternatives for its supply chain management switching to RFID can lead to enormous changes. All pros and cons need to be examined in detail, considering cost, productivity, flexibility as well as possible setbacks until the system reaches a stable phase. The management needs to get a good understanding of RFID and its possibilities.

If a company wants to use RFID it first has to be aware of the different types of transponders and the appropriate readers. As in the chapter “Transponder Overview” shown the read range, permeability, and the read speed are depending on the type of tag. Each scope of application needs its separate investigation regarding the appropriate tag type and reader.

### 2.8.1 RFID benefits for companies (Ferrer, Dew, & Apte, 2010)

A company may have different objectives. Some company goals which could profit from RFID are summed up as follows:

- Performance optimization and standardization
- Long term cost reduction
- Automating the value-adding process

RFID can improve the service quality and as a result, the performance in the company by:

- Reducing loss of inventory
- Increased safety and security
- Better identification process of objects

RFID may also improve the speed in a company and as a result its possible throughput by:

- Tracking possibilities – real time information regarding the position of an item
- Faster identification process

The flexibility of the company service can be improved by

- Faster identification of customers and their needs
- Self-service operations can be offered to the customers

Increased speed and flexibility of the process with the quality at least the same ultimately leads to the most important benefit of an appropriately used RFID system: lower costs.

Some very popular use cases regarding RFID and its advantages have already been mentioned in the section “RFID-applications”. For a more detailed look into applications used in companies please refer to (Ferrer, Dew, & Apte, 2010). It gives a good overview of RFID tags used in different companies with different needs. 22 cases were compared to each other showing the advantages and disadvantages of RFID used in this field.

## 2.8.2 RFID problems and weaknesses

Even though RFID has some great advantages it is important to think about its weaknesses as well in order to get a full understanding of the technology. Some points that have to be considered when it comes to RFID are (Maierhuber, 2013):

- RFID is susceptible to different forms of attacks that have been mentioned in the Chapter 2.6 already.
- The recycling process of RFID tags is very complicated. The biggest problem is that materials like aluminum, silicon and silver, which are the main components of a tag, cannot be recycled. An extraction of the tag from recyclable materials would mean deterioration in terms of cost and quality. (Sower, Bellah, Zelbst, & Green, 2013)
- RFID tags are more expensive compared to similar technologies (e.g. QR-Code, Barcode)
- RFID signals could influence other devices in their region (e.g. medical devices).

## 3 Near Field Communication (NFC)

Near Field Communication (NFC) can be defined as a contactless technology used for data exchange over short distances. The technology can be seen as a branch of RFID with the ability that a NFC device can switch between the roles of a reader and a transponder. The great advantage about NFC is that it is integrated into many smartphones which makes the technology available for everybody. This chapter provides an insight into the history of NFC, its basic concepts, and popular applications.

### 3.1 NFC-History

By taking a look at the history of Near Field Communication it has to be considered that the roots of NFC can be found in RFID technology.

Nevertheless, will start our lookback from the year 2002 when the name NFC has actually become public. That year Sony and NXP Semiconductors collaborated to create a technology inspired by RFID. (Langer & Roland, 2010)

In 2004 other cellular telephone companies (Nokia, Philips, and Sony) agreed to work together on this technology. For this purpose the NFC Forum was established. The aim was to create standards as well as to address security issues and the usability of NFC. One of the outcomes was that devices supporting NFC have to meet defined requirements set by the NFC Forum. In 2006 the first official specifications for NFC tags, smart posters, and smart tags were introduced by the NFC Forum. A tag shall be able to contain read-only or rewritable information and can be read by a NFC capable device once it is passed over the tag. In the same year the first NFC capable phone was presented by Nokia (6131). In January 2009 peer-to-peer standards were released which enabled the sending of pictures, music, videos, etc. to other NFC capable phones. The Samsung Nexus S was the first Android NFC device introduced by Samsung in 2010. (NearFieldCommunciation.org)

Nowadays the most important sectors of NFC are mobile payment, ticketing, and product information. The technology has not yet exhausted its potential. Even though its mayor sectors can be found in Europe, Asia, and Japan the United States is catching up rapidly. (Langer & Roland, 2010) (NearFieldCommunciation.org)

## 3.2 NFC Forum

The NFC Forum was formed 2004 as a non-profit organization with the goal to standardize the NFC technology and to enable its worldwide use. Meanwhile 16 specifications have been released by the forum. Whereas its original members have been leading mobile communications companies like NXP Semiconductors, Sony, Nokia, and Philips the forum has now more than 150 members, including manufacturers, developers, financial services, institutions, and others. (NFCForum, What it Does)

The main goals of the forum can be defined as (Langer & Roland, 2010):

- Standardization regarding the architecture
- Promotion of NFC in the development of products
- Ensure that products using the NFC technology commit to the standards defined by the forum
- Education with regard to NFC

Table 2 shows the 5 major member categories (including popular examples) with respect to their rights and annual dues.

	Members	Annual dues	Rights
Sponsor Members	<ul style="list-style-type: none"> <li>• Apple</li> <li>• Sony</li> <li>• Google Inc.</li> <li>• ...</li> </ul>	50.000 US\$	<ul style="list-style-type: none"> <li>• Most voting rights</li> <li>• Seat on the board of directors</li> </ul>
Principal Members	<ul style="list-style-type: none"> <li>• Canon Inc.</li> <li>• Hewlett Packard</li> <li>• Infineon Technologies</li> <li>• ...</li> </ul>	25.000 US\$	<ul style="list-style-type: none"> <li>• Voting rights regarding new standards</li> </ul>
Associate Members	<ul style="list-style-type: none"> <li>• Panasonic</li> <li>• Daimler AG</li> <li>• Toshiba Corporation</li> </ul>	10.000 US\$	<ul style="list-style-type: none"> <li>• Voting rights regarding new standards</li> </ul>
Implementer Members	<ul style="list-style-type: none"> <li>• BMW Group</li> <li>• Silicon Craft</li> <li>• Fujitsu Limited</li> <li>• ...</li> </ul>	5.000 US\$	<ul style="list-style-type: none"> <li>• No voting rights</li> </ul>
Non-Profit Members	<ul style="list-style-type: none"> <li>• Open Ticketing Institute</li> <li>• FH OÖ Forschungs- &amp; Entwicklungs-GmbH</li> <li>• Austrian Institute of Technology</li> </ul>	1.500 US\$	<ul style="list-style-type: none"> <li>• No voting rights</li> </ul>

Table 2: NFC forum members categories (NFCForum, Our Members)

## 3.3 NFC technology

NFC is a technology that enables a two-way interaction between electronic devices in a simple and safe way. The difference to RFID systems is that NFC devices can act as both readers and transponders. Such devices are able to work in active reader mode as well as in a passive transponder mode. (Langer & Roland, 2010)

NFC works on short-ranges (less than 4 centimeters) with a maximum communication speed of 424 kbps. A simple touch between two NFC capable devices enables a contactless transaction. It allows a clear assignment between reader and transponder. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

Another advantage of NFC is that it is based on existing standards, meaning that it can communicate with already existing contactless card infrastructures and RFID systems working with frequencies at 13.56 MHz. (Langer & Roland, 2010)

NFC has three different operating modes as described in (NFCForum, What it Does):

- Peer- to-Peer Mode
  - Communication between two NFC-devices
- Reader/Writer Mode
  - Communication with passive transponders
- Card Emulation Mode
  - Communication with RFID-readers

A deeper look into these three operation modes can be found in Chapter 3.3.6.

One big advantage of NFC is that it can handle multiple protocols, which indeed allows a developer to access the system in a variety of ways. The large amount of interfaces emphasizes that the applications and possibilities seem endless with NFC. The Protocol Stack of NFC is depicted in Figure 24.

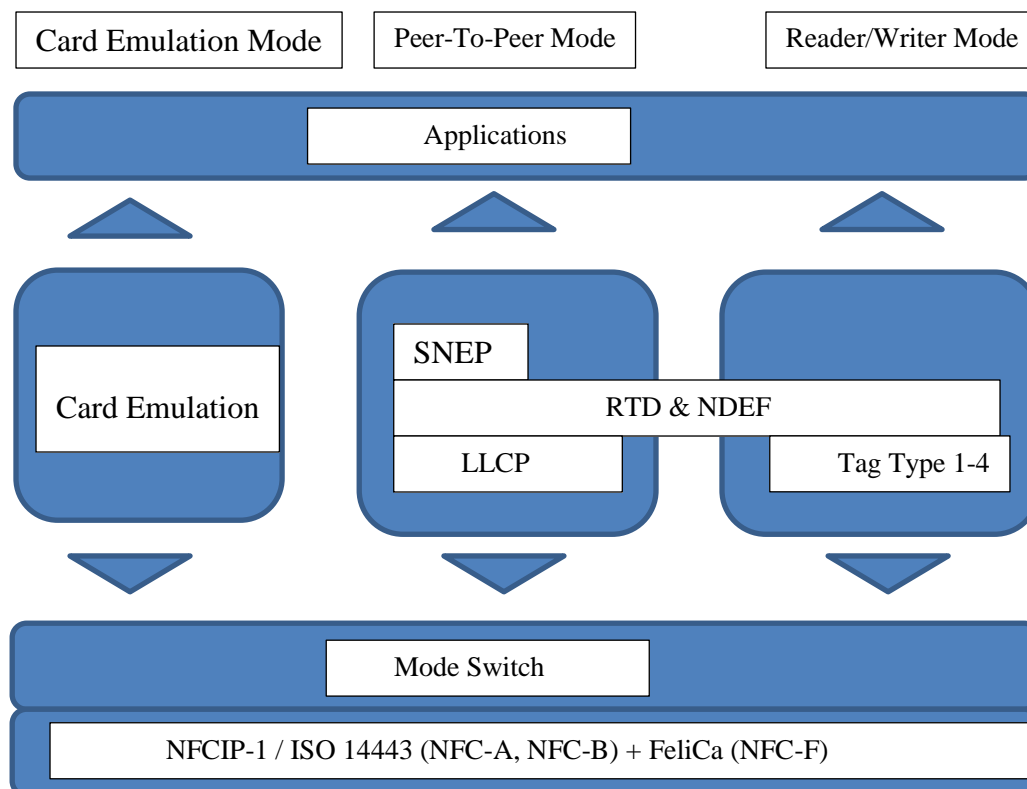


Figure 24: NFC protocol specifications (Keen, 2009)

The fact that NFC is capable of multiple protocols makes it a great technology for the user. He/she can use it in different applications based on several protocols. For a programmer however the protocols stack is quite complex because of a lot of standards supporting similar features. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

Depending on the mode that is used different protocols are needed. This chapter provides a deeper look into the different kinds of protocols and their purposes. Based on these protocols the supported modes of operation (Card Emulation, P2P and Reader/Writer) will be presented.

### 3.3.1 Near Field Communication Interface and Protocol (NFCIP)

The two basic standards used in NFC are NFCIP-1 (EcmaInternational, ECMA-340, 2013) and NFCIP-2 (EcmaInternational, ECMA-352, 2013).

NFCIP-1 is the base standard. It defines the communication modes and the basic technical features, whereas NFCIP-2 defines the sequence of mode-switching for a selected or detected communication mode. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

### *3.3.1.1 NFCIP-1 (ECMA-340 and ISO 18092)*

NFCIP-1 is a norm that standardizes the communication mode for NFC using inductive coupled devices at a frequency of 13.56 MHz and data rates of 106, 212 and 424 kbps. The standard also defines the two communication modes NFC is capable of: active and passive mode. (Rackley, 2007)

The standard defines the specification for (EcmaInternational, ECMA-340, 2013):

- Modulation schemas
- Data coding schemas
- Transfer speeds
- Frame format of the RF interface
- Data collision handling

The standard defines a simple transport protocol as well, which includes methods for activation, deactivation and data exchange. (EcmaInternational, ECMA-340, 2013)

### *3.3.1.2 NFCIP-2 (ECMA-352 and ISO 21481)*

This standard was defined as an extension to NFCIP-1. The NFCIP-2 standard distinguishes between the three different modes of operation a device is using. It supports proximity cards and vicinity cards in addition to the NFCIP-1 standard. The standard also defines the communication mode switching mechanism. (EcmaInternational, ECMA-352, 2013) (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

The supported communication standards are (Langer & Roland, 2010):

- NFC mode
  - Devices as describe in the NFCIP-1 standard
- Proximity Integrated Circuit Card (PICC) mode
  - Passive transponder with ranges of up to 10 cm
- Proximity Coupling Device (PCD) mode
  - Active devices with ranges of up to 10 cm
- Vicinity Coupling Device (VCD) mode
  - Active devices with ranges of up to 1 m

NFCIP-2 devices are compatible to other systems as they have to implement functions for all described supported communication modes.

### 3.3.2 Logical Link Control Protocol (LLCP)

LLCP is a protocol standard introduced by the NFC Forum. It is based on the industry standard IEEE 80.2, which was designed as a support for small applications with limited data transport requirements. LLCP defines an OSI Layer-2 protocol and is used in Peer-To-Peer communication of two NFC capable devices. It allows the data exchange between two devices. (NFCForum, NFC Forum Technical Specifications)

Different to other protocols, like the Data Exchange Protocol, LLCP enables a bidirectional communication. Initiator and target are equal communication partners, where each of them can start the data transfer. (Langer & Roland, 2010)

### 3.3.3 NFC Data Exchange Format (NDEF)

The NDEF is a binary format specification introduced by the NFC Forum. It clearly defines the format and rules how the data transfer between NFC capable devices or tags should work. It does not matter if the data is exchanged between two devices or between a NFC tag and a device. A common data format ensures that the same structures can be used. Protocols like LLCP or SNEP for example exchange messages in NDEF format. (Langer & Roland, 2010)

The use of NDEF messages in NFC is one difference compared to RFID. Whereas RFID messages do not need to have a specified format all NFC devices are working with NDEF. Consequently a NFC capable device knows what to do with a received message, especially in case of well-known record types (RTDs). (Igoe, Coleman, & Jepson, 2014)

A NDEF message can consist of one or multiple NDEF records.

#### 3.3.3.1 *NDEF Record*

A NDEF record consists of a header and its payload. The header gives information regarding the type of the record, its unique ID, and the length of the message. The payload length of a NDEF records is limited to  $2^{32}-1$  Byte. However, the messages can be chained together that's why they in theory have a variable length. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

Nevertheless, the messages tend to be shorter than longer since NFC is designed on the principle “tag and go”. The structure of an NDEF record is described in Figure 25.



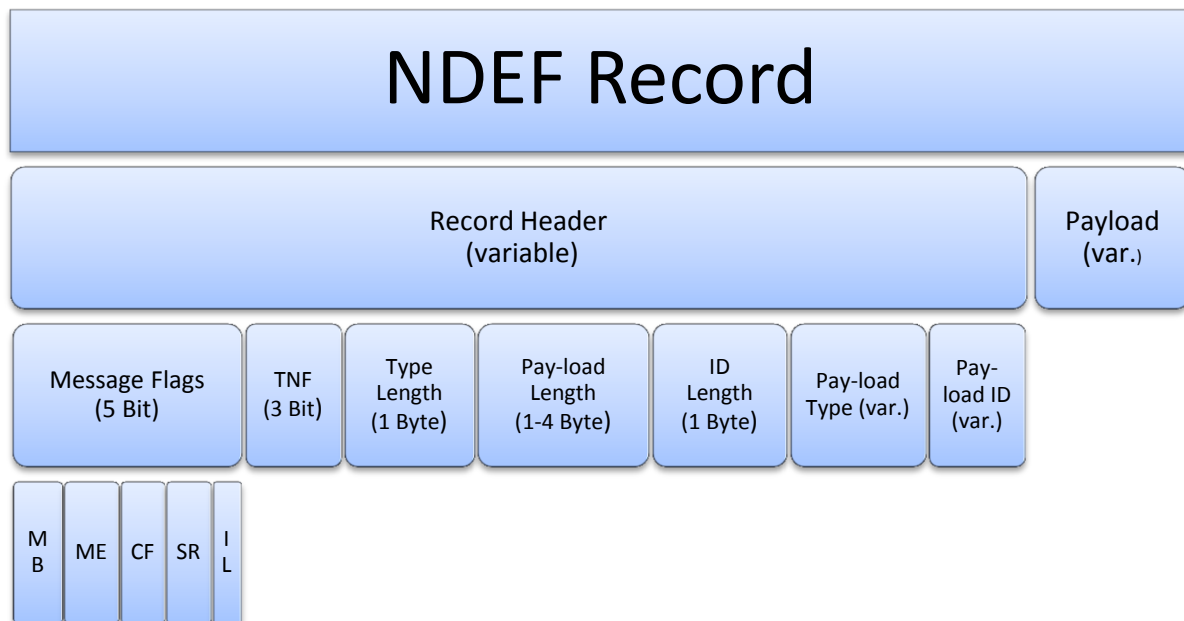


Figure 25: NDEF message structure (Coskun, Ok, & Ozdenizci, *Professional NFC Application Development for Android*, 2013)

The first five bits contained in the record header are flags each consisting of 1-bit information. Further information's in the header are defined through the type format, its payload, and its length. Table 3 gives a brief overview regarding the NDEF record fields.

Message Begin (MB)	
	Identifies the first NDEF record in the message if set
Message End (ME)	
	Identifies the last NDEF record in the message if set
Chunk Flag (CF)	
	Identifies that the message is divided (i.e. chunked) over the current and the next NDEF record
Short Record (SR)	
	Identifies a short record field. The standard payload length is 32 bit. If this flag is set to 1 the payload length is 8 bit.
ID Length Present (IL)	
	Identifies that the record contains identification information.
Type Name Format (TNF) Field	
	<p>The TNF is a 3 bit value containing information regarding the record type. It shows which kind of information can be expected in the record.</p> <p>The content of this field is part of the NDEF specification</p> <ul style="list-style-type: none"> <li>• 0x00 empty record <ul style="list-style-type: none"> <li>○ The record has no type, no ID, and no payload</li> <li>○ All length values are set to 0</li> </ul> </li> <li>• 0x01 NFC Forum well-known record <ul style="list-style-type: none"> <li>○ The identifier “nfc” indicates that a well-known record type is used</li> <li>○ The name format for RTD types is used.</li> <li>○ This type of record is most commonly used.</li> </ul> </li> <li>• 0x02 MIME Media Record <ul style="list-style-type: none"> <li>○ Multipurpose Internet Mail Extension (MIME) record</li> </ul> </li> <li>• 0x03 Absolute URI Record <ul style="list-style-type: none"> <li>○ Uniform Resource Identifier (URI) record</li> </ul> </li> <li>• 0x04 External Record <ul style="list-style-type: none"> <li>○ NFC Forum external type record based on RTD specification</li> </ul> </li> <li>• 0x05 Unknown Record <ul style="list-style-type: none"> <li>○ Often used if an information is stored in multiple records. Only the first record contains the type information, all others have the TNF set to unknown</li> </ul> </li> <li>• 0x06 Unchanged Record <ul style="list-style-type: none"> <li>○ This type is reserved for further extensions.</li> </ul> </li> </ul>
Type Length (1 Byte)	
	8 bit value containing the length of the type

Payload Length (1-4 Byte)	
	<ul style="list-style-type: none"> <li>• Contains the length of the payload</li> <li>• 8 bit value if SR = 1</li> <li>• 32 bit value if SR=0</li> </ul>
ID Length (1 Byte)	
	<ul style="list-style-type: none"> <li>• 8 bit value containing the length of the ID</li> <li>• Only present if IL Flag is 1</li> </ul>
Payload Type	
	<ul style="list-style-type: none"> <li>• Variable length</li> <li>• Describes the type of the record, following the criteria of the TNF</li> <li>• For a well-known record type (TNF 01) the Payload Type could be <ul style="list-style-type: none"> <li>○ “T” for Text</li> <li>○ “U” for URI</li> <li>○ “Sp” for Smart Poster</li> <li>○ “Sig” for Signature</li> </ul> </li> <li>• A MIME type (TNF 02) could have a payload type <ul style="list-style-type: none"> <li>○ “text/html”</li> <li>○ “text/json”</li> <li>○ “image/gif”</li> <li>○ etc.</li> </ul> </li> <li>• The payload type of an absolute URI type (TNF 03) would be a literal URI</li> <li>• An example for a payload type of an external type (TNF 04) could be something like “android.com:pkg”</li> </ul>
Payload ID	
	<ul style="list-style-type: none"> <li>• Variable length</li> <li>• URI that identifies the record</li> <li>• Optional field</li> <li>• Examples: <ul style="list-style-type: none"> <li>○ 0x01: <a href="http://www">http://www</a>.</li> <li>○ 0x02: <a href="https://www">https://www</a>.</li> <li>○ 0x05: tel:</li> <li>○ 0x06: mailto:</li> </ul> </li> </ul>
Payload	
	<ul style="list-style-type: none"> <li>• Data to be transmitted or a part of the data if multiple chunks exist</li> <li>• The data has to meet the requirements of the format defined in the type-field</li> </ul>

Table 3: NDEF record fields description (Langer & Roland, 2010) (adafruit) (Igoe, Coleman, & Jepson, 2014)

### 3.3.3.1.1 Record Type Definition (RTD)

The Record Type Definition is a specification introduced by the NFC Forum. The NDEF specification is used to define the data format and structure of a message. However NDEF does not define any detailed guidelines regarding the handling of the record types. (NFCForum, NFC Record Type Definition (RTD) Technical Specification, 2006)

The RTD specification defines guidelines regarding the handling of record types to ensure that a message can be exchanged appropriate between NFC devices or a NFC reader and a tag (Langer & Roland, 2010). Beside the data structure and the handling of well-known record types the specification also gives guidelines regarding the creation of external types (Igoe, Coleman, & Jepson, 2014).

A NDEF message with the defined TNF 0x01 (well-known record) or 0x04 (external record) needs to follow the guidelines of RTD.

#### 3.3.3.1.1.1 RTD Types

The specification defines guidelines for 4 specific well-known record types (TNF 0x01) as described in Table 4. The payload type in an NDEF message identifies the used RTD type.

NFC Text RTD
<ul style="list-style-type: none"> <li>• Is used for efficient text encapsulating in multiple languages.</li> <li>• There are no criteria defined how to handle this type of record.</li> <li>• Text RTDs can be combined with other RTDs.</li> </ul>
NFC URI RTD
<ul style="list-style-type: none"> <li>• Is used for storing of Uniform Resource Identifiers.</li> <li>• A URI can be             <ul style="list-style-type: none"> <li>○ An email address</li> <li>○ A web address</li> <li>○ A phone number</li> <li>○ Identification codes like an Electronic Product Code</li> </ul> </li> <li>• This type of RTD can be combined with other RTDs (URI RTDs are an important part of Smart Poster RTDs for example)</li> </ul>
NFC Smart Poster RTD
<ul style="list-style-type: none"> <li>• This RTD is an extension of the URI RTD, combined with other RTDs (mostly text RTDs containing meta-information)</li> <li>• Smart Poster RTDs can be exchanged between NFC devices</li> <li>• Mostly used for advertising posters. A touch with a smartphone allows a user to access more information regarding an advertisement (opening a web-page, sending an SMS, etc.)</li> </ul>
NFC Signature RTD
<ul style="list-style-type: none"> <li>• Used to sign the other RTDs in a message. A Signature RTD record signs all records from the start of the message (or after another signature RTD) up to its direct predecessor record. An example is shown in Figure 26.</li> <li>• This type of RTDs are very important, as they give applications the opportunity to check the integrity and the identity of an NDEF record by its signature</li> </ul>

Table 4: RTD types (Langer & Roland, 2010) (NFCForum, Record Type Definition Technical Specifications)

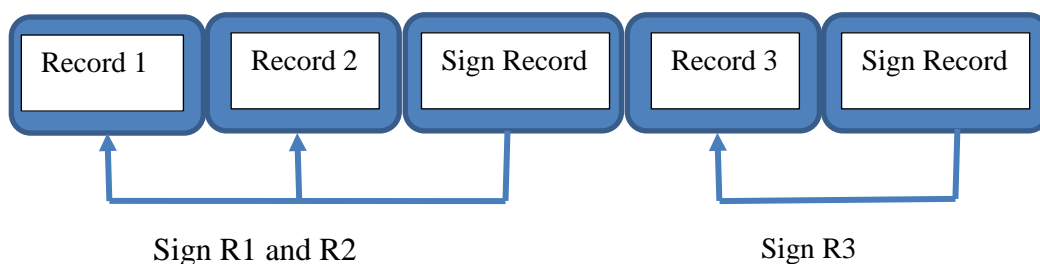


Figure 26: Example Sign Record (Langer & Roland, 2010)

### 3.3.3.1.2 NDEF Message Example

The example in Table 5 gives a short overview of how a NDEF-message would look like, based on an URI record type for <http://www.nfc-forum.org>.

7	6	5	4	3	2	1	0
<b>MB</b>	<b>ME</b>	<b>CF</b>	<b>SR</b>	<b>IL</b>	<b>TNF</b>		
1	1	0	1	0	0	0	1
Message Begin YES	Message End YES	Chunk Flag NO: Message not divided	Short Record YES: Payload length is 8 Bit	ID Length Present NO	Type Name Format 001: NFC Forum Well-Known Record		
<b>Type Length</b>							
0x01							
Type Length: 1 Bit							
<b>Payload Length</b>							
0x13							
Payload Length: 19 Bit							
<b>ID Length</b>							

0x0
ID Length: not present because of IL = 0
<b>Payload Type</b>
0x55
ASCII: “U” => Payload Type is “URI”
<b>Payload ID</b>
0x01
0x01 URI Identifier: “http://www.”
<b>Payload:</b>
0x6E 0x66 0x63 0x2D 0x66
0x6F 0x72 0x75 0x6D 0x2E
0x6F 0x72 0x67
Payload: “nfc-forum.org”

Table 5: NDEF-Message example

The message consists of one NDEF record. This is obvious as the MB and the ME flags are set to 1. The CF flag shows that the message is not chunked – meaning it consist of only one NDEF message. The TNF is an important field as it indicates that the record type that is transferred is a well-known record type, whereas the payload type itself tells us that we are dealing with an URI record type with the identifier code “http://www.” defined in the payload ID.

### 3.3.4 NFC Simple NDEF Exchange Protocol (SNEP)

The SNEP protocol is a stateless request/response protocol. It is mostly used in smartphones for peer-to-peer communication. SNEP enables two NFC devices to exchange NDEF messages.

The basic process can be defined as following (Tiedemann):

- A request by the initiator is sent to the target.
- The target processes the incoming request.
- A response is returned to the client.

SNEP does not define how the exchange has to be handled, like LLCP, the handling is operating system specific (e.g. Android Beam for Android). Due to the fact that SNEP lays over LLCP it is also possible to run other protocols for data exchange over the data link layer of LLCP. (Coskun, Ok, & Ozdenizci, Near Field Communication (NFC): From Theory to Practice, 2011)

### 3.3.5 Tag Types

Tags are passive storage elements. To ensure compatibility NFC tags are based on RFID tags. NDEF records can be written to tags. According to the fact that the tags are based on RFID, an RFID reader should be able to read them as well. (Langer & Roland, 2010)

Older RFID readers however do not support the NDEF standard, which means, they should be able to identify the tag and to read it's UID but they cannot read the data encoded on the tag (Igoe, Coleman, & Jepson, 2014).

The different types of messages that can be stored on a tag have already been described before. Beside a simple text or an URI even commands can be saved on a tag that trigger an action on a phone after reading the tag (e.g. turn off/on the sound at a touch).

The NFC Forum distinguishes between 4 tag types from 1 to 4 (described in Table 6). Depending on the use case, the needed memory, data rate, cost and other criteria's each type has its pro and cons. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)



Type 1
<ul style="list-style-type: none"> <li>• This tag type is based on the ISO/IEC 14443 Type A standard</li> <li>• Readable/writable</li> <li>• Memory up to 1 kB (can be expanded to 2 kB)</li> <li>• Data rate up to 106 kbps</li> <li>• The costs for this type of tag are very low. This makes it usable for a lot applications requiring small memory (e.g. URL storage)</li> <li>• The disadvantage is that the tag only offers a collision detection at initialization but no anti-collision. Because of this multiple tag types can't be initialized at once</li> <li>• Example: Topaz</li> </ul>
Type 2
<ul style="list-style-type: none"> <li>• Based on ISO/IEC 14443 Type A standard</li> <li>• Readable/writable</li> <li>• Memory up to 2kB</li> <li>• Data rate up to 106 kbps</li> <li>• Tag costs are low                             <ul style="list-style-type: none"> <li>○ This tag type is capable of anti-collision detection – multiple tags can be detected by a reader if they are in its read range</li> </ul> </li> <li>• Example: NXP Mifare</li> </ul>
Type 3
<ul style="list-style-type: none"> <li>• Based on ISO 18092 standard</li> <li>• Readable/writable</li> <li>• Memory up to 1 MB</li> <li>• Communication speed up to 212 kbps or 424 kbps</li> <li>• High tag costs</li> <li>• Capable of anti-collision detection</li> <li>• Example: Sony FeliCa</li> </ul>
Type 4
<ul style="list-style-type: none"> <li>• Based on ISO/IEC 14443 Type A and Type B standard</li> <li>• Readable/writable</li> <li>• Memory up to 64 KB</li> <li>• Communication speed between 106, 212 and 424 kbps</li> <li>• Tag costs in medium to high level</li> <li>• Capable of anti-collision detection</li> <li>• Example: NXP DESFire</li> </ul>

Table 6: NFC Tag types (Langer & Roland, 2010) (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

### 3.3.6 NFC operation modes

In NFC we can distinguish between 4 main roles according to (NearFieldCommunication.org):

- Reader/Writer
  - The R/W is typically a card reader or smartphone working in active mode.
  - The active device sends signals and receives information's.
- Card
  - A card is the passive device (e.g. a NFC tag or a passive phone acting in Card Emulation mode)
  - The R/W sends requests to the card.
  - The card answers the instructions.
- Initiator
  - The initiator is the NFC device that is responsible for connection setup in Peer-To-Peer mode.
- Target
  - In P2P mode the target is the device that receives instructions by the initiator and answers with the requested information's.

NFC distinguishes also between two communication modes described in (Macias & Wyatt, 2014):

- Active Mode
  - In active Mode, both initiator and target have their own power supply. The initiator generates its radio frequency (RF) field, sends a request, and turns the RF field off. The target in revers generates an own RF field for the response.
  - Example: 2 phones
- Passive Mode
  - This mode is similar to the concept of RFID. The target gets its power from the initiator. The transmission from tag to reader happens with load modulation. This mode is compatible to RFID standards.
  - Example: Phone & RFID tagged poster

Based on the used protocols NFC can act in three different modes (Langer & Roland, 2010):

- Peer-To-Peer
  - Used for communication between two NFC capable devices (e.g. 2 smartphones), where one device acts as initiator and the other one as target.
- Reader/Writer
  - Used for communication with a passive NFC tag or with other contactless chip cards
- Card-Emulation
  - In this mode the NFC device acts as a contactless Smart Card. It is used for communication with RFID readers, where the NFC device is the transponder.

### *3.3.6.1 Peer-To-Peer mode (P2P)*

The Peer-To-Peer mode in NFC is used for data-transfer between two NFC capable devices. The communication mode in P2P is always between two active devices. (Igoe, Coleman, & Jepson, 2014)

The data exchange between the devices is based on the Logical-Link-Control Protocol (LLCP) and the Simple NDEF Exchange Protocol (SNEP). The two protocols do not define how the exchange should be handled or how the GUI needs to look like for the user. Each application has to implement this on its own. The most popular implementation for P2P is Android Beam. In Android Beam two smartphones need to be put together with their backsides. If NFC is activated and if the NFC radio detects another NFC capable device the “touch to beam” interface appears. The user can confirm the information sharing with one touch. This information is then sent via P2P with NDEF messages to the other device. (Igoe, Coleman, & Jepson, 2014)

### 3.3.6.1.1 P2P protocol stack

The protocol stack architecture of NFC Peer-To-Peer mode can be summed up as shown in Figure 27.

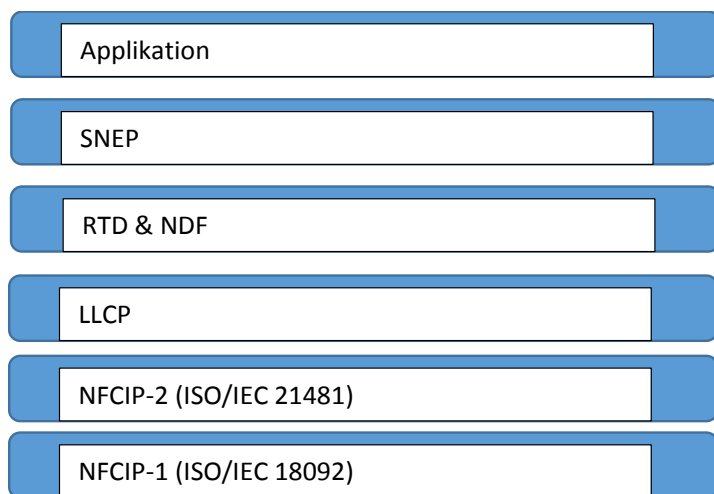


Figure 27: NFC P2P protocol stack (Langer & Roland, 2010) (SmartCardAlliance, 2012)

The P2P mode is based on the NFCIP-1 standard, which defines the basic standards for NFC, like the frequency rate, communication rate and its communication modes.

One device acts as initiator, the other one as target. Whether a device enters the mode as initiator or as target is defined in the NFCIP-2 standard (EcmaInternational, ECMA-352, 2013):

- 1) If an external RF field can be detected the device has to enter the NFC mode as target.
- 2) If no external RF field can be detected, but the NFC mode is selected, the device has to enter the NFC mode as initiator.

LLCP is used for the data transfer between two devices. It is the ground for P2P applications as it enables a bidirectional connection between two NFC devices. SNEP is used as it allows the exchange of NDEF messages over LLCP. On the top of this protocols use case specific applications are used. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

### 3.3.6.1.2 P2P participants

The P2P-mode is used for data transfer between two active devices. As can be seen in Figure 28 the principle is simple. The initiator sends or requests data and the target responds.



- 1) Initiator creates a RM-Field
- 2) Initiator sends data/requests to the target
- 3) Initiator turns off its RM-Field
- 4) The target creates its RM-Field
- 5) The target sends data
- 6) The target turns its RM-Field off

Figure 28: P2P communication between two active devices

One of the most popular NFC devices is a smartphone. To make it capable of NFC it has to have some specific components. Which components and how they work together is shown in Figure 29.

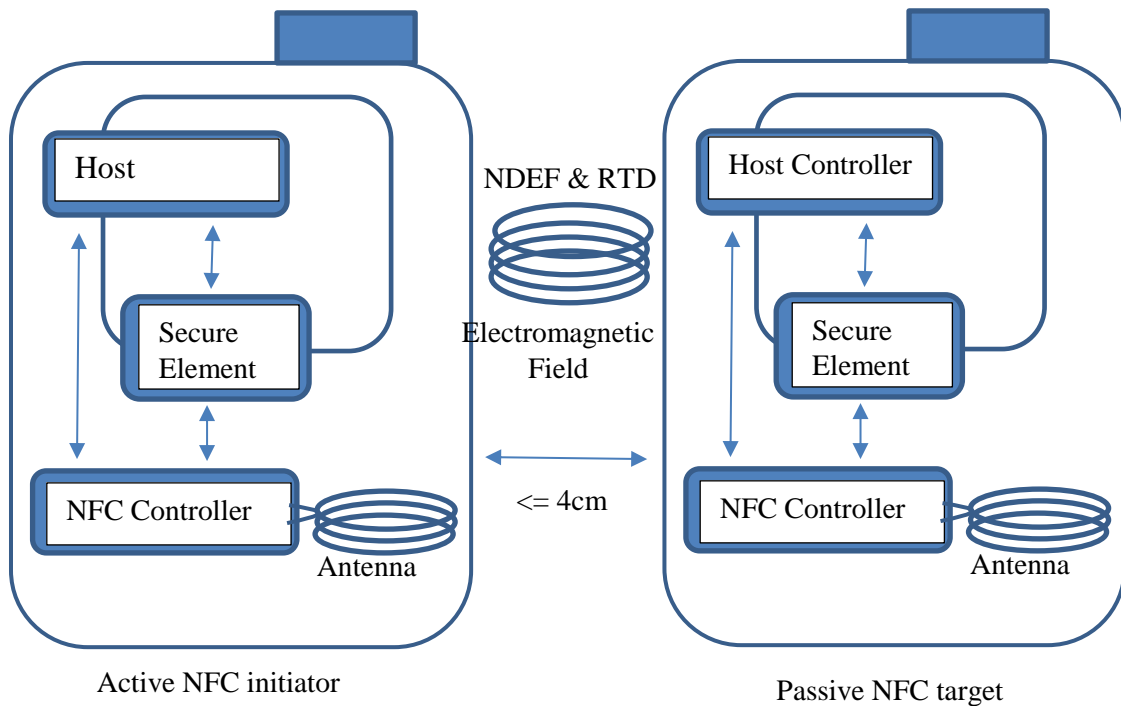


Figure 29: Principle of P2P communication (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

According to (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013) the main NFC participants in a mobile phone are:

- The NFC interface consisting of
  - NFC Antenna
    - An antenna is the basic module in NFC to enable the receiving and the transmitting of a signal
  - NFC Controller
    - Also called “Contactless Front-End (CLF)”
      - Modulates and demodulates the incoming and outgoing signal
      - Is capable of NFCIP-1 and other standards which enable the communication in all 3 NFC modes.
  - Secure Element (SE) described in (Langer & Roland, 2010) as:
    - The SE is the element allowing applets to run in a secure environment. This component is also used in smart cards.
    - In a smartphone you can find a SE at least one time.
    - The SE is connected to the NFC controller.
    - Especially in case of mobile payment and critical data the SE is the most important component in performing transactions.
- Host Controller
  - The “heart” of the mobile phone
  - Application Execution Environment (AEE)
  - Is linked to the NFC Controller over an interface

### 3.3.6.1.3 Touch to share

Even though it is not the main purpose of NFC, it is very easy to exchange information between two mobile phones with it. This chapter gives a short example of how the exchange of data could look like.

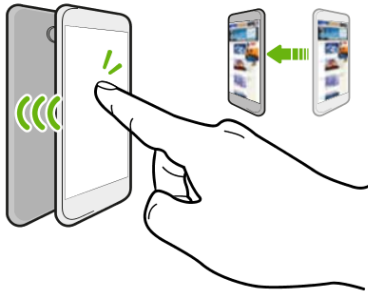


Figure 30: NFC p2p mode (touch to share) <sup>8</sup>

If two mobile phones are capable of NFC it provides a very good alternative for exchanging data. Suppose two persons (A and B) would like to exchange their contact information. They do not need to type in name and number by their self any more. By doing it in the “NFC-way” A would open his/her contacts and open the contact he/she wants to share (in that case the own contact). Now A and B put their phones together (typically back to back) as shown in Figure 30. The application determines on its own what should be sent. After a confirmation by A (typically a touch) the content gets transferred to the phone of B. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

Sending big amounts of data is also possible with NFC. Nevertheless, regarding to the fact that the participants would need to hold their phones together till the exchange is finished, it is used for exchanging smaller data. An alternative for sending bigger data over NFC would be the combination with Bluetooth, which is also called “NFC pairing” and is described in the next section. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

### 3.3.6.1.4 Touch and Connect (Negotiated Handover)

On the one hand exchanging data like photos, audio-files or even bigger data can get sluggish with NFC. On the other hand technologies that allow a faster data rate and a larger read range like WLAN or Bluetooth mostly have the problem that you have to configure it on both devices correctly before you can start sharing. NFC pairing is a good alternative to this problem as it combines the comfort of NFC with the speed of another contactless technology.

NFC provides a Connection Handover Specification. It is used for establishing a connection with other wireless technologies. This specification uses NDEF messages for the communication. (Langer & Roland, 2010)

---

<sup>8</sup> <http://www.htc.com/sea/support/htc-desire-600-dual-sim/howto/373822.html>

Example: Two participants A and B want to share a photo (Igoe, Coleman, & Jepson, 2014):

- A (initiator device) selects the corresponding photo
- A and B (target device) put their devices together and A confirms the exchange with a touch
- The initiator sends now a Handover Request to the target and all alternative technologies that could be used by it for sending the data.
- The target answers with a Handover Selector Record including its own alternative carriers.
- The initiator chooses one of the carriers if a match can be found.
- If for example both devices are capable of Bluetooth the initiator would select this technology as handover carrier.
- After that the target sent its configuration data to the initiator
- The initiator initiates the pairing of the devices

The advantage is obvious. The participating users do not need to exchange passwords or any other configuration data. Bluetooth is used without the need to turn it on or to give a separate permission for the pairing of the devices. The NFC interface communicates with the operating system, asks it to turn an alternative carrier device on, and does the pairing for the user.



### 3.3.6.2 Reader/Writer (R/W) mode

This mode is used for interaction with NFC Forum tags. An active NCF capable device can read data from a tag and handle it afterward or write data to writable tags.

The Reader/Writer mode opens up a very wide range of applications. It is backward compatible to already existing RFID systems, where the NFC device can be used as reader. Mobile ticketing, smart posters, access control are just a few of examples where this mode can be used.

#### 3.3.6.2.1 Reader/Writer protocol stack

The protocol stack architecture of the Reader/Writer mode is summed up in Figure 31:

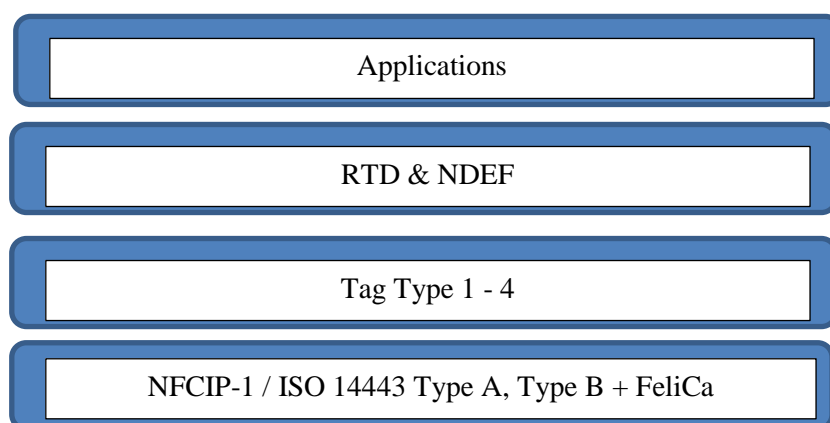


Figure 31: Reader/Writer protocol stack (Coskun, Ok, & Ozdenizci, *Professional NFC Application Development for Android*, 2013)

The foundation of Reader/Writer tags is the NFCIP-1 standard with its communication configuration and its collision detection (Single Device Detection).

NFC Forum tags are readable/writable tags with different read ranges, memory, anti-collision handling, and manufacturers. A NFC capable device working in Reader/Writer mode should be able to interact with the different tag types. The data on a tag is structured in NDEF data format with the use of RTDs. Depending on the NDEF record type that is stored on the tag the information can be accessible to all NFC capable devices (TNF\_WELL\_KNOWN record) or just to a specific application (TNF\_EXTERNAL\_TYPE). (Coskun, Ok, & Ozdenizci, *Professional NFC Application Development for Android*, 2013)

#### 3.3.6.2.2 Reader/Writer participants

The R/W mode is used for data transfer between an active devices and a passive tag. As can be seen in Figure 32 and Figure 33 the principle is simple. The initiator sends or requests data, the target responds.



- 1) Initiator creates a RM field
- 2) Initiator sends data/requests to the target
- 3) The target responses using load modulation

Figure 32: Reader/Writer mode communication between an active and a passive component

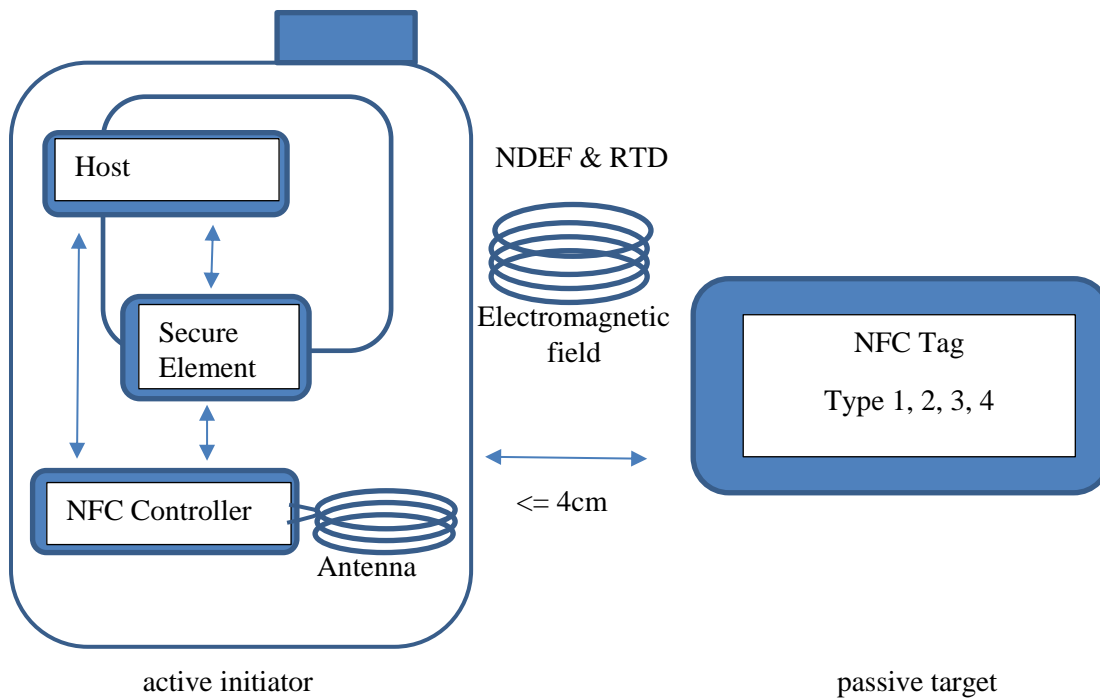


Figure 33: participants of reader/writer communication (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

The mobile device as active initiator and its components have already been described in Chapter 3.3.6.1.2.

### 3.3.6.2.3 Touch and Connect (Static Handover)

Due to the fact, that the Reader/Writer mode has the same problem as the Peer-to-Peer mode when it comes to data transfer of bigger data, NFC provides the Connection Handover Specification also for the communication with passive devices. The Static Handover enables the data transfer via Bluetooth, WLAN or another carrier over NFC.

An example could be a device that is capable of Bluetooth but not of NFC, like for example a printer or a smartphone without NFC. A NFC tag containing a Handover Select NDEF message with the configuration parameters needed for a connection via Bluetooth can be attached to such a printer/smartphone. An active device would now be able to read this configuration from the tag and to send data to the printer/smartphone over Bluetooth.

A good use case is a public WiFi Spot. The configuration parameters can be saved on tags that are easy to reach. In this way it is possible to share the WiFi credentials enabling users to use the WLAN without any need of configuration.

This connection process has some disadvantages as well:

- The configuration parameters on the tag are static
- According to the example above the printer would need to have Bluetooth activated permanently.
- Saving connection parameters on a tag means making them public. This is only rational for free interfaces that are already meant to be available for free.

(Igoe, Coleman, & Jepson, 2014)

### 3.3.6.2.4 Touch and Display

When it comes to tags, the “touch and display” use case is the first that comes to mind. Especially Smart Posters make use of this functionality. NFC tags on a poster contain information that is presented by a simple touch.

The typical NDEF Record type for smart posters would be a WELL\_KNOWN\_TYPE as this kind of information is meant to be accessible for free. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

### 3.3.6.2.5 Touch and Call / Touch and Send

Tags can also be used to trigger process like making a call, sending a SMS, a mail, or a geolocation for example. Even shopping via NFC tags is a possibility. A NFC tag placed on a product could be read by an application that allows you to make a purchase. Since such instructions are meant to be read by specific applications which then trigger further steps, an EXTERNAL\_TYPE record would be used for tags. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

### 3.3.6.3 Card Emulation mode

This mode enables the communication between a NFC enabled device and a RFID reader or a NFC device working in R/W mode. In Card Emulation mode the mobile phone is working like a passive, contactless smart card.

The mode is optional, which means a mobile phone that is capable of NFC does not need to support the Card Emulation mode as well. (Langer & Roland, 2010)

The advantage that the mode offers is that a mobile phone can emulate multiple smart cards, no matter if the purpose is access control, identification or a payment process. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

#### 3.3.6.3.1 Card Emulation protocol stack

The protocol stack architecture of the Card Emulation mode is shown in Figure 34.

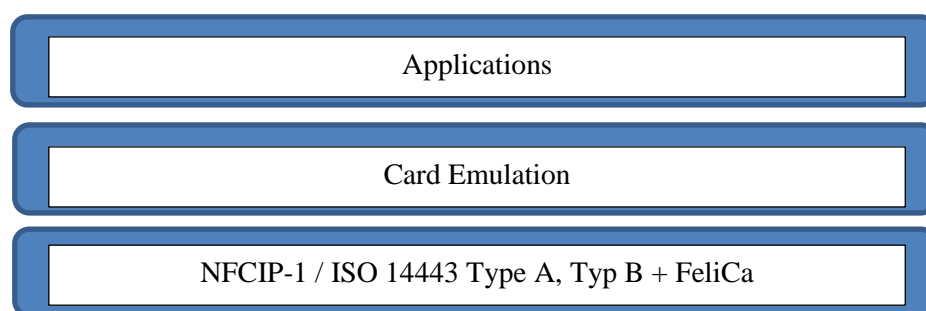


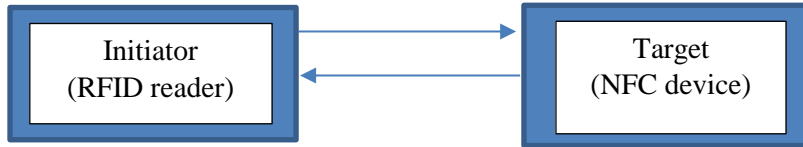
Figure 34: Card Emulation protocol stack (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

Like in the other two modes the grounding of the Card Emulation mode is the NFCIP-1 specification with its functionalities.

Depending on the NFC chip the functionalities available in Card Emulation mode can differ from device to device. In the most cases the smart cards are emulated by a secure element (SE). When the mobile phone is held to an RFID reader all data is passed to the SE. For the transaction process no application is need. Only for the confirmation to the user an application can be integrated. (Langer & Roland, 2010)

### 3.3.6.3.2 Card Emulation participants

The communication between the phone and the reader works basically like in the Reader/Writer mode except the fact that the mobile phone is the target. A visual example of the communication is given in Figure 35 and Figure 36.



- 1) Initiator creates a RM field
- 2) Initiator sends data/requests to the target
- 3) The target responds using load modulation

Figure 35: Card Emulation mode communication between an active and a passive component

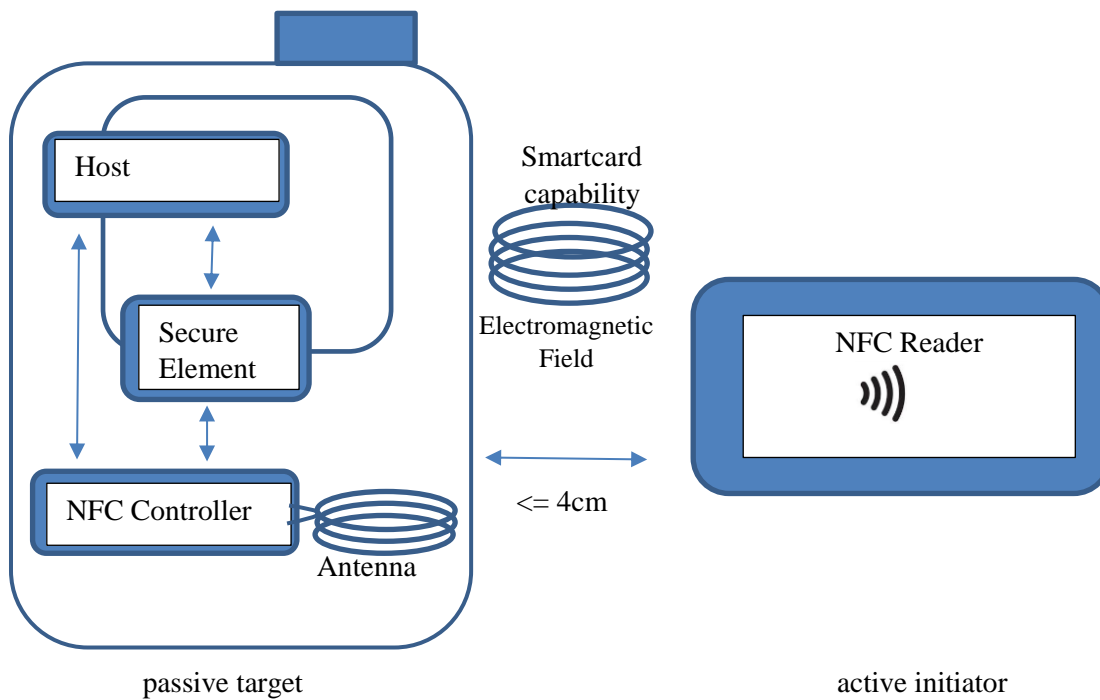


Figure 36: Card Emulation participants (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

#### 3.3.6.3.3 Touch and Pay

The most popular use case regarding the Card Emulation mode is cashless payment, also known as *Proximity Payment*. Today's mobile phones have already become a good alternative to a lot of devices (e.g. MP3-Player, Gameboy, PC, etc.). With NFC they are able to replace payment cards and subsequently our consideration of the conventional purse.

Even though the standard procedure for mobile payment would be to touch a card reader with your phone and to enter a passcode, the passcode isn't really needed for the transaction.

The possibilities are almost unlimited in the money transfer. Not only the process of paying is possible, also the debit from ATMs is possible with NFC. Only a NFC reader is needed to be attached to the ATM. Transferring money to a friend? No problem – NFC in P2P mode can make it possible. Another advantage may be that receipts could be saved automatically on the smartphone which could give you in turn a better overview of your outgoings. Personalized advertising would reach a further step. Of course, in case of monitoring and observation the same advantages could be interpreted as disadvantages as well. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

#### 3.3.6.3.4 Touch and show your ticket

Mobile ticketing is another important representative of the Card Emulation mode. Instead of buying at the counter it can be bought online and saved on the phone. Touching a card reader with the smart phone gives the access to a concert, bus, train, subway-station, etc.

### 3.3.7 NFC with SoC and Microprocessor

The first thing that comes to mind talking about active devices in NFC are smartphones and maybe their bigger versions, tablets. Especially applications that rely on additional electronic or mechanical components can benefit from microprocessors like Arduino with associated NFC modules or system-on-a-chip (SoC) devices like the Raspberry Pi. (Igoe, Coleman, & Jepson, 2014)

This section gives a short overview of the Raspberry Pi and its possibilities regarding the connection of a NFC reader/writer.

#### 3.3.7.1.1 Raspberry Pi

The Raspberry Pi was first introduced 2012 by the Raspberry Pi Foundation. The system-on-a-chip device is a small computer, with a price of about 35 €. The device was primarily designed for learning purpose. The amazing thing about it is that it can be used in multiple ways (Richardson & Wallace, 2014):

- As personal computer. Connected to a display, the Raspberry Pi can be used for watching movies or surfing in the web.
- To learn the basic concepts of a computer and how to program it.
- For electronic projects. The Pi has General Purpose Input and Output (GPIO) pins directly on board which makes it easy to connect it to electronic components.

Even though it does not have its own internal storage SD cards can be used as flash memory to save data on it. Even the operating system is saved on a SD card. Due to built-in Ethernet it can even be used for networking. (Richardson & Wallace, 2014)

The Pi comes in different models, which differ in their on-board equipment as shown in Table 7.

	RP Model A	RP Model A+	RP (2) Model B	RP Model B+	RP Zero
CPU	700 MHz		700 MHz / 900 MHz (RP2)		1 GHz
Memory	256 MB		512 MB / 1 GB	512 MB	512 MB
USB Port	1		2/4	4	Micro-USB
Ethernet Port	No	No	Yes	Yes	No
Power source	Micro USB power (5V)				
Video and Audio output	HDMI (rev 1.3 & 1.4)			Mini HDMI socket	

Table 7: Raspberry Pi models overview (RaspberryPiFoundation, raspberrypi) (RaspberryPiFoundation, Raspberrypi.org)

### 3.3.7.1.2 Raspberry Pi with NFC and RFID

There exist different modules on the market that can be used as extension to the Pi in order to enable RFID or NFC on it.

#### 3.3.7.1.2.1 NFC over USB

The SCL 3711<sup>9</sup> for example is a contactless NFC reader and writer that can be connected via USB port. It is not PI-specific since it can be used for any computer with an USB port. It supports the OS: Windows, Mac OS X and Linux. The supported tags are:

- ISO/IEC 14443-3 Type A and B
- ISO/IEC 14443-4
- Mifare
- FeliCa
- NFC Forum Tags (1,2,3,4)

#### 3.3.7.1.2.2 NFC over shield or breakout board

As an alternative to a NFC R/W over USB, a shield can be used to enable NFC reading and writing with a Pi. A PN532 NFC shield is a good example regarding such modules. A PN532 chip for example is used in the most smartphones that are enabling NFC. The most NFC readers and writers, like the SCL 3711 are not capable of a tag emulation mode, in contrast to the PN532. (adafruit)

---

<sup>9</sup><http://www.shopnfc.it/en/nfc-readers-writers/59-scl3711-contactless-reader-nfc-enabling-accessory.html>



## 4 NFC compared to other contactless Technologies

The following section gives an overview of different contactless technologies with regard to their major use cases and the potential of NFC for this kind of usage.

What makes NFC particular is that it can be used in different areas. The following examples compare NFC with the contactless technologies RFID, Smart Cards, Barcodes, and QR Codes. Without considering the advantages and disadvantages it can already be said that NFC provides opportunities to be used as a substitute for all of this technologies. However, considering price, labor, and benefits the use of NFC is not always recommendable. What is possible and what is actually useful is far apart in case of NFC.

Before starting the comparison NFC specific properties such as frequency rate, read rate, data rate, etc. are summed up in Figure 37 for a better overview.

### Frequency rate

- 13,56 MHz

### Data rate

- 424 Kbit/s

### Read range

- up to 10 cm (better: <=4cm)

### Reusability

- Rewritable tags

### Durrability

- Can be read even after pollution

### Power consumption

- very low

### Operation Mode

- Read/Write
- Peer-to-Peer
- Card Emulation

### Areas

- Payment process
- Access control
- ticketing
- sharing data

### Tags

- 4 Types

### Max. Memory

- depending on the type
- up to 4 kByte total (~3 kB available)

*Figure 37: Summary regarding NFC properties*

## 4.1 Barcode

A Barcode is probably the most familiar technology when it comes to automated identification systems. The first experiments regarding the Barcode we know today can be found in year 1949. The first scanned product containing a Barcode on it was a pack of Wrigley's chewing gums in the year 1974. The basic idea was to get customers more quickly through the supermarket checkout. In the 1950s first attempts were made to apply this technology also for automatic recognition in industries. (Rosistem), (Weightman, 2015)

### 4.1.1 Universal Product Code (UPC)

The UPC is a convention regarding the structure of a Barcode formed by the Uniform Code Council (UCC). A UPC consists of 12 digits and is divided into the Barcode that is read by a scanner and a number under the Barcode that can be read by a person. (Bhasker, 2001)

A Barcode is a pattern of bars that encodes information. Depending on the order and the thickness of the bars different information will be read by a scanner. Usually the Barcode encodes an ID which in turn refers to a product. The product specific information's are stored in a database where the ID on the Barcode is the key.

The structure of a Barcode can be divided into 3 main parts (Finkenzeller & Müller, 2010):

- Company ID (6 digits)
  - Refers to a manufacturer.
  - All products of a manufacturer have the same 6 digits at the beginning.
- Item number (5 digits)
  - This is the ID that references to a real product.
- Check Digit (1 digit)
  - Used to show the reader whether the Barcode has been read correctly.



Figure 38: Example Barcode (© 1994 – 2016 Barcodes, Inc)<sup>10</sup>

Based on the barcode from Figure 38 the following example shows how to calculate the Check Digit (BarcodesInc):

- 1) Calculate all odd numbers:
  - $8 + 1 + 3 + 0 + 0 + 0 = 12$
- 2) Multiply result from 1) with 3
  - $12 * 3 = 24$
- 3) Calculate all even numbers:
  - $1 + 2 + 4 + 0 + 0 = 7$
- 4) Calculate the sum from 2) and 3)
  - $24 + 7 = 31$
- 5) Determine the number that is needed to get a multiple of 10 from the result in 4)
  - $31 + 9 = 40$
- 6) The check digit needs to be 9

A Barcode reader scans the alternating bars with a red light. Based on the reflections an algorithm is used to convert this bars in a machine text and finally to identify the product itself. (BarcodesInc)

---

<sup>10</sup> <https://www.barcodesinc.com/faq/#what>

## 4.2 Quick Response (QR) Code

The QR Code can be seen as a successor of Barcode. It contains squares, called modules in a two-dimensional way. Because of this representation the QR Code is able to save more information than a standard barcode. QR Codes can even store downloadable content. The most common use case for this technology is to store URLs on it. The roots of today's QR Code can be found in 1994. (Unitag)

The QR Code has become very popular in last years. The main reason is that it can be read by a smartphone. Companies have discovered this advantage as a good, simple, and cheap way of marketing. By saving a URL to a QR Code and printing this on a product a customer can access the information stored on the code very easily. Another advantage of QR Codes is that they can be created very easily. Nowadays a lot of websites exist offering QR Code creation even for free. (WEBSCAN)

Beside the QR Code other 2-dimensional barcodes exist as well, like for example the Data matrix or the Microsoft Tag. (Unitag)

## 4.3 Smart Card

A Smart Card can be defined as a plastic card of a standardized size containing a microchip on it. We can distinguish between two types of Smart Cards:

- Memory card
  - Typically: EEPROM-cards
  - Can be compared with a tag with read and/or write access
- Processor card
  - Such cards contain a microcontroller which controls specific functionalities

Regarding the communication mode we can distinguish Smart Cards again in (Langer & Roland, 2010):

- Contact cards
- Contactless cards
- Mix between contact and contactless cards

We can distinguish between different standards used for contactless Smart Cards. The standards can be distinguished regarding their read range and their operating frequency. The three Smart Card types: Proximity Coupling, Vicinity Coupling, and FeliCa are based on the same standards that are used for NFC devices. They are operating at a frequency of 13.56 MHz with a read range of about 1 cm. This is also the reason that a NFC capable phone working in card emulation mode can be read by some Smart Card readers. (Coskun, Ok, & Ozdenizci, Near Field Communication (NFC): From Theory to Practice, 2011)

## 4.4 Popular use cases with respect to NFC

The following section compares the previously described technologies RFID, Barcode, QR Code and Smart Cards with NFC regarding their most popular field of application.

### 4.4.1 Tracking systems

A tracking system is used for observing issues. Its main purpose is to track movements of items or persons in order to get a better understanding of their position, processing, and other issues. When it comes to supply chain management, object identification and processing is an important topic. Especially real time information's and automatic identification is getting more and more to the fore. Nowadays, mainly RFID and Barcodes are used for such issues. Objects that need to be tracked are equipped with a Barcode or an RFID tag. The difference regarding the identification is that Barcodes needs to be scanned one by one, in most cases by a person, whereas multiple RFID tags can be read by stationary readers in a warehouse over a long read range at a time. Normally the tag only carries an ID on it referring to an entry in a database which contains the object-specific data that is of interest. Suppose for example a full shopping cart. In case of Barcodes you need to take all items out of the cart and scan one after another to get the correct price. Using passive RFID tags attached to goods a reader can scan all items in a few seconds without the need to empty the cart. Because of its usability over long ranges and its speed when it comes to identifying multiple objects in a short period, RFID is excellent for tracking systems. However RFID isn't the best solution always. If we again think of the shopping cart – does it make sense to attach a tag to each article even if the tag costs about 0,10€? How about loose items like for example fruits? We still need to scan them separately if we don't want to have a tag on each apple. The example shows that RFID may be a good solution for a lot of problems but possible disadvantages regarding the resulting price and potential over-optimization could be an outcome. Especially for small companies RFID could be the step in such a direction.

The biggest advantage about Barcodes is that they are easy to handle, cheap, and easy to produce. Barcodes are already used all over the world in supply chain management.

Since RFID tags in supply chain management need to work over wide ranges NFC would not be a good replacement. However Barcodes need to be scanned from short distances. However, NFC tags would probably serve the same needs as Barcodes.

Using NFC tags instead of Barcodes in supply chain management could mean:

- Time saving, since reading NFC tags is much faster than scanning Barcodes.
- Cost increase, since NFC tags are more expensive than Barcodes.
- NFC tags have more storage capacity. However, this is not necessary if storing only an ID.
- The read range is almost the same for both technologies.

A transition from barcodes to NFC would mean more costs for companies as they would need to buy new readers or NFC capable smartphones, pay more for the tags, and they would have to face possible problems regarding the usability during the initial stage. (Adaptalift, 2012)

Table 8 gives an overview of the advantages and disadvantages from RFID, Barcodes and NFC regarding their use for tracking systems.

Which technology should be used depends on the circumstances. Before using RFID a company needs to investigate its processes and to think about the possible consequences. If the value that comes out from the usage of RFID is big enough, higher tag costs will be an investment that pays off.

Considering the Pros and Cons of NFC for tracing systems it could be said, that especially in regard to the tag costs in contrast to a Barcode, no benefit would justify the use of NFC nowadays in companies. But, tag costs are already sinking, which is why the use of NFC in place of barcodes could be considered as very likely if this trend continues.

RFID	Barcode	NFC
<ul style="list-style-type: none"> <li>• <b>PRO</b> <ul style="list-style-type: none"> <li>• Object specific data can be stored on a tag</li> <li>• Location of an object can be determined</li> <li>• Collection of environmental information possible</li> <li>• Identification and reading can be automated because of fixed readers</li> <li>• Multiple tags can be read</li> <li>• Identification process over long distance</li> <li>• Fast read rate</li> <li>• Read/write possible</li> <li>• Very resistant</li> </ul> </li> <li>• <b>CON</b> <ul style="list-style-type: none"> <li>• More expensive than Barcodes (tag costs of about 0,10 € + costs for reader and infrastructure)</li> <li>• Permeability depends on the used material</li> <li>• Tag collision possible</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>PRO</b> <ul style="list-style-type: none"> <li>• Known and proven technology that is widely used</li> <li>• Easy to use</li> <li>• Cheap</li> <li>• Very good accuracy</li> </ul> </li> <li>• <b>CON</b> <ul style="list-style-type: none"> <li>• Need to scan one Barcode after another from a short read range</li> <li>• Not really resistant - easy to damage - not readable even after pollution</li> <li>• no read/write possible</li> <li>• a Barcode can only save the following information: manufacturer + product</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>PRO</b> <ul style="list-style-type: none"> <li>• Object specific data can be stored on a tag</li> <li>• Collection of environmental information possible</li> <li>• Fast read rate</li> <li>• Read/write possible</li> <li>• Very resistant</li> </ul> </li> <li>• <b>CON</b> <ul style="list-style-type: none"> <li>• More expensive than Barcodes (tag costs of about 0,10 € + costs for reader and infrastructure)</li> <li>• Permeability depends on the used material</li> <li>• Tag collision possible</li> <li>• Need to scan tags one by one from a short read range</li> </ul> </li> </ul>

Table 8: Comparison between RFID, Barcode and NFC for the use in tracking systems (Adaptalift, 2012)



## 4.4.2 Marketing

Marketing is getting more and more into focus nowadays. The customer's desire for information about a product, its origin, and component is increasing more and more.

With regard to the discussed contactless technologies it can be said with absolute certainty that the QR Code is the only one that has found its own importance in the world of marketing. QR Codes can be found anywhere a business wants to draw attention to a product or a company (product packaging, menus in restaurants, visit cards, etc.)

The main advantages of the QR Code are (QRCodeStickers):

- can be produced very easily
- low costs
- ability to store more than just a ID on the Code (example: URL)
- can be read with every smartphone that has a camera and a QR-Code reader installed

Qrstuff.com<sup>11</sup> is a very popular site offering the generation of a QR Code for free. You can choose between different types of data like for example: URL, YouTube Video, Google Maps Location, Message, Telephone Number, etc.

The greatest problem regarding QR Codes is that the standard customer is not really interested in scanning it. Most people don't even know what a QR Code is. Nevertheless, QR Codes including downloadable content like for example coupons or product details still have great potential.

Possible marketing places for QR Codes are (DeMers, 2014):

- business cards
- Brochures
- Product packaging
- Restaurant menus
- Clothing
- Billboards
- Store windows
- Every places where you want to draw attention to a product and/or a company

Table 9 gives an overview of the advantages and disadvantages from QR Code and NFC regarding their usage for marketing issues.

---

<sup>11</sup> <http://www.qrstuff.com/>

QR Code	NFC
<ul style="list-style-type: none"> <li>• <b>PRO</b> <ul style="list-style-type: none"> <li>• Easy and cheap in production since the most QR Code generators are for free.</li> <li>• A QR Code does not take lot space and can be printed almost everywhere.</li> <li>• Can be read by any smartphone with a camera and an installed QR Code reader.</li> <li>• Higher read range than NFC.</li> </ul> </li> <li>• <b>CON</b> <ul style="list-style-type: none"> <li>• An application is needed for QR Code scanning.</li> <li>• A standard customer does not have a QR Code scanner installed or does not even know what a QR Code is.</li> <li>• QR Code scanning takes much time.</li> <li>• Security issues since you don't know where a code is leading you before scanning it.</li> <li>• Permanent - if the content needs to be changed a new QR Code has to be created.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>PRO</b> <ul style="list-style-type: none"> <li>• Reading over a simple and short tap - especially when it comes to reading of small data like for example an URL.</li> <li>• If the tag is not considered to be handled by a special application that needs to be pre-installed the NFC reader of the smartphone is enough for reading.</li> <li>• More secure transactions.</li> <li>• The contained information can be changed easily.</li> </ul> </li> <li>• <b>CON</b> <ul style="list-style-type: none"> <li>• Can only be read by NFC capable phones.</li> <li>• Higher costs</li> <li>• Short read range</li> </ul> </li> </ul>

Table 9: comparison of QR-Code and NFC regarding the use for marketing issues (QRCodeStickers), (Qrky)

QR Codes could be replaced by NFC tags by time, especially when it comes to issues like security, comfortability, and robustness. However, the full potential of QR Codes has not yet been exploited. Its possibilities regarding marketing purposes have been recognized, however, the proper use is still in its infancy.

The QR Code is a technology that can bring many benefits but it is still under construction. A fact that supports this statement is that still no agreement exists regarding the content that should be saved on a QR Code in case of marketing purpose. However, as the use of QR Code is virtually free, you can at least experiment well with it. The switch to a more expensive technology like NFC that do not offer more advantages does not seem to be promising. (Qrky)

Basically the main disadvantage of QR Codes is that scanning of a code takes a while and the customer needs a special QR Code scanner installed. NFC on the other hand is not available on all smartphones for now. Technological process will not be limited to NFC only, meaning, NFC will get more and more available in new smartphones, but smartphone cameras will probably get better as well. (Qrky) So you can assume that from the time where NFC will

be available on all smartphones the built-in cameras will also be much better, and therefore a faster scan of QR Codes will be possible.

Other reasons which are in favor of the preference of QR Codes in marketing sector:

- NFC means higher costs without additional advantages.
- A QR Code can easily be printed on a product packaging whereas the inclusion of NFC chips on millions of packages, which are thrown away afterward would mean dissipation.

Off course there are as well reasons to prefer NFC over QR Codes. An example would be the use of ever-changing data (Nearfieldcommunication). Printing a new QR Code every-time instead of reprogramming a NFC tag could be more expensive after a time. Another reason that speaks for the preference for NFC could be if the robustness of the code/tags must be in foreground. The use of QR Codes in tangible goods is for example not recommended. Consider, for example, a QR Code which is located on a piece of clothing that is being worn. On the one hand the person wearing the piece of clothing needs to stand still to ensure a successful scanning by a scanner on the other hand clothes get washed, folded, dirty, etc. – a QR Code would be useless after the first use.

Summing up, we can draw that both technologies have their advantages and disadvantages. Depending on the application area, the budget, the robustness, the reading speed, and the required amount of memory preference can be drawn.

### 4.4.3 Entrance Systems

The times where we used a key for entering a hotel room, our workplace, or university are over. Nowadays contactless Smart Cards are used for entrance systems.

Electronic entrance systems typically use readers that are working on a frequency rate of 125 kHz and/or 13.56 MHz (Finkenzeller & Müller, 2010). Compared to traditional solutions, like using keys, electronic entrance systems have a lot of advantages. Like for example if a user needs to have access to multiple buildings but not to all. Saving this information on a Smart Card is much easier, faster, and cheaper than giving the person multiple keys for different buildings.

Basically we can distinguish between two types of electronic entrance systems as described in (Finkenzeller & Müller, 2010):

- Online system
  - Used if the access authorization needs to be individually handled based on the person who wants to enter (= different people have different access rights to different buildings).
  - Even a simple read-only tag with an ID on it would be enough to serve the need.
  - A database in reader's background gets accessed to check the entry permissions regarding the read ID.
  - It is very easy to add or remove access rights.
  - If a tag or Smart Card gets lost a person's access right can be removed very easy and moved to another ID.
  - Such systems are often used in companies.
- Offline system
  - This kind of systems does not have a database in its background.
  - The keys that get access are saved in a list by the system itself.
  - The tag on the other side saves all the keys to the rooms it delivers access to.
  - When the tag is held to the transponder the keys on the tag are compared with those in the terminals list. If a match can be found access is permitted.
  - In order to make changes to the access rights the transponder needs to be reprogramed.
  - Used in hotels for room access.

When it comes to entrance systems NFC could be a very good solution. Considering the fact that the most entrance systems are already working at a frequency of 13.56 MHz no changes would be needed for NFC technology. As the smartphone itself can emulate a transponder access can be granted via touching the reader by the phone of the customer.

A possible scenario for an online System with NFC could be (Langer & Roland, 2010):

- The application used for the entrance system is installed on the employee's phone.
- After installation the employee automatically gets access to the buildings for which he/she has an authorization in the central database.
- Further changes regarding the access policies can be done without the employee's phone.
- Advantages:
  - No keys/tags/Smart Cards needed
  - Saves time and money

A possible use scenario for an offline system with NFC could be (Langer & Roland, 2010):

- A customer wants to reserve a room at a hotel.
- The booking is done over the hotels homepage.
- After the reservation the customer gets the key for the hotel room via SMS or E-mail.
- The delivered authorization keys are saved in his/her phone.
- The customer gets access to the hotel room over tapping the reader with his/her phone.
- Such a system could bring advantages like:
  - Shorter check in and check out times
  - Promote customer loyalty
  - Save additional tags/keys/Smart Cards

## 4.5 Comparison contactless technologies

Table 10 shows a summary of the above sections. It gives an overview of the described technologies and their usability for different applications. As can be seen NFC as well as RFID are most versatile regarding their field of usage.

Use case	Description	RFID	NFC	QR Code	Bar-code	Smart Card
Tracking systems	Tracking and identifying multiple objects in short time (E.g. Supply Chain Management, Animal Tracking)	✓	✗	✗	✗	✗
	Identifying an object after another to get object-specific information (ID saved on object – application in background delivers the information)	✓	✓	—	✓	✗
Entrance Systems	Get access to a building	✓	✓	—	—	✓
Ticketing	Get access based on an electronic ticket (e.g. transporting)	✓	✓	—	—	✓
Paying systems	Pay cashless	✓	✓	✗	✗	✓
Electronic toll collection	Cashless tolling systems that enable a car to pay and pass a toll without stopping	✓	✗	✗	✗	✗
Antitheft systems	Electronic security to prevent theft	✓	—	✗	✗	✗
Data exchange	Exchange images, contact cards, etc.	✗	✓	✗	✗	✗
Data storage	Store URLs, text or even sensitive data on a tag and get access to this data	✓	✓	—	✗	—
Marketing	Provide more information about a product or company on the product itself or on flyers, posters etc.	✗	✓	✓	—	✗

Table 10: RFID, NFC, QR Code, Barcode usability for different use cases

## 5 Practical Part – NFCQuiz-App

Even though NFC is a technology that is known mainly from the payment and ticketing sector there exist some studies regarding the potential of NFC for completely different use cases. As has already been described in the theoretical part NFC provides a far untapped potential for a variety of applications. In the field of learning, NFC can for example be used as a supporting tool for distributing or sharing documents and info-material in a course. Another use case could be the proof of identity in exams. (Maierhuber, 2013)

Due to the card-emulation and reader-mode in mobile phones even a scenario where the student writes the whole exam on his/her phone (multiple-choice questions), submits it and automatically gets his/her mark over NFC would be possible.

The following chapter is dedicated to the usage of Near Field Communication in the field of game based learning. The motivation was to test the potential and the usability of NFC in the educational area through the use of “prototyping” as solution strategy. The outcome of the research was an Android-based quiz application (“NFCQuiz”) using different NFC approaches for data exchange.

The application is supposed to have the following advantages:

- No internet access is needed for participation. The whole game works offline.
  - No need to store the questions on a web server,
  - to exchange the URL with the contributing players, or
  - to download a question-set
- By using re-writable tags there are basically no limits in terms of reuse
  - The player gets an additional interactive effect by holding the phones together for synchronization which in turn keeps the participants interested. The feeling you get when playing with cards or tokens can be partially emulated.
  - Control over the questions and answers
    - The game can be used to repeat learning content in a fun way.
    - Even multiple choice tests could be conducted this way. The result could be available immediately.

## 5.1 Motivation

The goal was to explore the possibilities of NFC regarding its implementation and usability on a smartphone.

Nowadays about 617 million NFC enabled devices are shipped per year (Boden, 2016). The expectation is that in two years NFC will be available in two from tree phones (IHS, 2014).

However some manufacturers still refuse to include NFC into their devices. Motorola for example don't want to implement a technology until it finds greater use. Apple on the other hand is supporting NFC finally but only as a support of Apply Pay since they do not see other purposes still. (Segan, 2012)

Different NFC capable operating systems are available on the market until now according to (NFCWorld, 2016):

- Android (since Version 2.3)
- Windows Mobile (since Version 6), Windows Phone (since Version 7.5)
- BlackBerry OS (since BBOS 7.0)
- Symbian (since Anna)
  
- IOS (since iPhone 6 but with restrictions)
  - iPhone 6, iPhone 6 Plus, Watch

Based on the fact that

- the most NFC enabled smartphones are based on Android OS,
- the widespread of Android phones,
- the author herself is passionate about Android smartphones, and is even owning a NFC capable smartphone

it was obvious that Android will be the used operating system for the prototype.



## 5.2 Android Basics

The following section gives a short overview of Android implementation and specially its support regarding NFC with respect to the implementation of NFCQuiz.

The official Integrated Development Environment (IDE) for Android is the Android Studio which was introduced in 2013. The IDE includes all relevant plugins needed for Android application development (e.g. Android Software Development Kit (SDK), platform tools, emulator, etc.). (AndroidDevelopers, Meet Android Studio)

Even though different environments can be chosen for android development, NFCQuiz was implemented in Android Studio as it provides a great usability.

NFC is supported in Android since API level 9 by providing the *android.nfc package*. However, since the most functionality has been introduced in API level 10 this is also the API level that should at least be used when it comes to NFC programming for Android. The classes and methods used for NFC support can be found in two packages (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013):

- android.nfc
  - read and write NDEF messages
  - peer-to-peer exchange
- android.nfc.tech
  - used for accessing the raw bytes of a tag that do not contain NDEF records

### 5.2.1 Android Manifest

The AndroidManifest file is mandatory for each android application. This file is saved in the application root directory and contains important information for the Android system like (AndroidDevelopers, App Manifest):

- Package name which is used as an identifier for the application
- API version that is at least needed to start the application
- Application name and icon which are presented to the user
- Contained components (activities, services, broadcast receiver, etc.)
- Permissions that are needed

To be able to use NFC in an application it is important to give the application the permission to handle NFC Intents in the AndroidManifest, as shown in Code Snippet 1.

```
<uses-permission android:name="android.permission.NFC"/>
```

*Code Snippet 1: set NFC permission in Android Manifest*

If the application needs to be able to discover NDEF tags the `minSdkVersion` needs to be set at least to 10, since the API level 9 does not support all needed NFC classes and methods as mentioned before. In Android 4.4 (`SdkVersion` 19) an extension for NFC was presented enabling the use of the card emulation mode without a secure element. This extension allows every Android application to emulate a card and subsequently to talk with the NFC reader directly. In this way it is possible to enable a bidirectional communication between two devices over NFC. To be able to exchange messages between two or more devices over NFC the `minSdkVersion` needs to be set at least to 19. This is also the setting that was used for “NFCQuiz” as it works in Card Emulation mode. Code Snippet 2 shows how to set the `minSdkVersion` in the `AndroidManifest`.

```
<uses-sdk android:minSdkVersion="19"/>
```

*Code Snippet 2: defining the minSDKVersion*

Code Snippet 3 shows how to define the application to be available exclusively for NFC devices in the manifest file. Only users with a NFC capable phone will be able to see and download the app from the store. (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

```
<uses-feature android:name="android.hardware.nfc"
  android:required="true" />
```

*Code Snippet 3: define NFC as needed hardware feature*

## 5.2.2 Intent

Intents are objects that enable a communication between applications. Over Intents other Activities can be called. As described in (AndroidDevelopers, Android Developers) Intents can be defined in two ways:

- Explicitly - by knowing the name of the Activity
  - Example: Application with two Activities where the first Activity starts the second Activity directly by its name.
- Implicitly - by defining the action that should be handled
  - Example: Sending a picture without knowing which application can handle this. The action `ACTION_SET` is used to define that the Activity wants to send a photo. The component that is used to do this is either started by Androids system directly (if only one application exists that can handle this Intent) or the user gets an application chooser presented and can decide which application should be used to handle the action (if multiple applications exist that can handle this Intent).

An Intent Filter is used to define the types of Intents that can be handled by an Activity, Service or Broadcast. (AndroidDevelopers, <intent-filter>)

A very popular Intent Filter is the one defining the main entry point of the application. An example of this filter is shown in Code Snippet 4. The action MAIN defines the main entry. The category LAUNCHER is used to define that the icon of the Activity should be presented in the application launcher.

```
<activity
  <intent-filter>
    <action android:name="android.intent.action.MAIN" />
    <category android:name="android.intent.category.LAUNCHER" />
  </intent-filter>
```

*Code Snippet 4: Android Manifest from NFCQuiz-Application. Intent-filter to define main-activity for app launcher*

If a NFC tag is discovered the type of the tag and its payload are encapsulated to an Intent. Androids system is now looking for an application to start that can handle the tag. Different scenarios are possible (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013):

- If only one application is register for this kind of tag this application will be started by Androids system.
- If multiple applications are registered for the same type the app launcher will be presented. The user can choose which application should be started.
- If no application is registered for the Intent nothing will happen.

An Intent Filter should be defined as specific as possible to avoid the app chooser dialog. In terms of NFC three Intents with descending priority can be distinguished (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013):

1) ACTION\_NDEF\_DISCOVERED

- If a NDEF-tag is discovered and only one application exists that is using the NDEF\_DISCOVERED Intent this Activity is started.

2) ACTION\_TECH\_DISCOVERED

- If a NDEF-tag is discovered and no Activity exists that can handle NDEF\_DISCOVERED or if the discovered tag does not contain NDEF data Androids system is looking for an Activity that can handle the TECH\_DISCOVERED Intent.
- In order to use this Intent Filter an Activity needs to define the tech types it refers to.

3) ACTION\_TAG\_DISCOVERED

- Activities containing an Intent Filter for TAG\_DISCOVERED will be called only if no other Activity can handle the discovered tag.

Figure 39 shows how Androids system is handling a discovered tag.

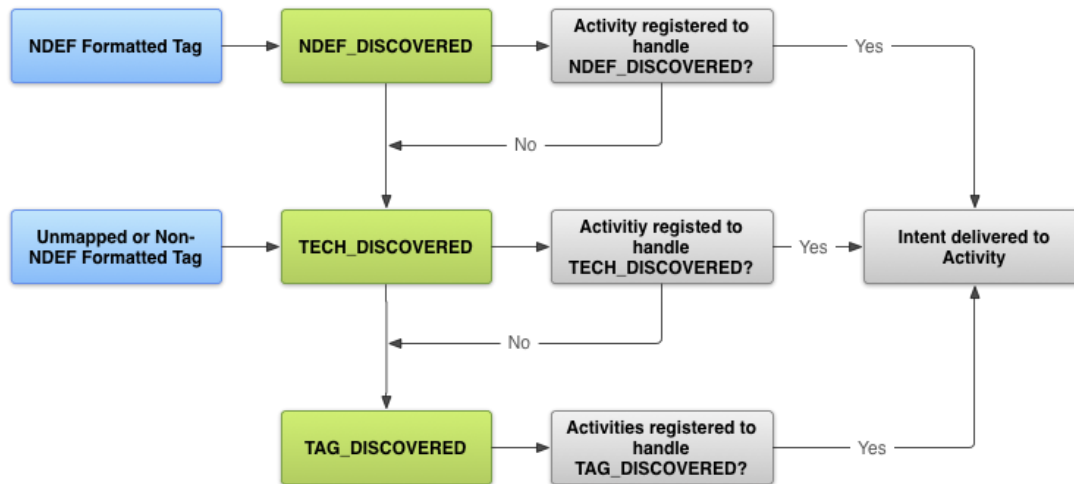


Figure 39: Activity chooser sequence for discovered tag (AndroidDevelopers, NFC Basics)

Code Snippet 5 shows how to define an Intent Filter for the action NDEF\_DISCOVERED. If a NDEF-tag is discovered containing a MIME type record of type text/plain this Activity will be started.

```

<intent-filter>
  <action android:name="android.nfc.action.NDEF_DISCOVERED"/>
  <category android:name="android.intent.category.DEFAULT"/>
  <data android:mimeType="text/plain"/>
</intent-filter>

```

Code Snippet 5: defining an Intent-Filter with respect to an AAR on a discovered NDEF tag (AndroidDevelopers, NFC Basics, kein Datum)

### 5.2.3 NFC Adapter

The NfcAdapter class is the representation of the phones NFC controller. It is essential for working with NFC capable applications. The function `getDefaultAdapter` returns the devices adapter. If the phone is not NFC capable `getDefaultAdapter` will return null. It is recommended to do the check in the `onCreate`-method of all Activities that are using NFC. Since NFC support is crucial for “NFCQuiz” further work is not possible if NFC is not available. Code Snippet 6 gives an example of how to retrieve the adapter. (AndroidDevelopers, Android Developers) (Chen, 2011)

```

mNfcAdapter = NfcAdapter.getDefaultAdapter(this);
if (myNfcAdapter == null)
  Toast.makeText(this,"NFC not supported", Toast.LENGTH_SHORT).show();
else if(!mNfcAdapter.isEnabled())
  Toast.makeText(this,"Enable NFC", Toast.LENGTH_SHORT).show();

```

Code Snippet 6: retrieve NFC adapter

## 5.2.4 Reading NDEF message from tag or beam

This section is dedicated to reading data in Peer-To-Peer mode and Reader/Writer mode with respect to NDEF messages. Reading data in Card Emulation mode is described in the section 5.2.6 Host Card Emulation (HCE). A NDEF message can contain one or more NDEF records, whereas every record consists of a header and a payload. The detailed format of NDEF messages has already been described in section 3.3.3 NFC Data Exchange Format (NDEF). In case of “NFCQuiz” plain text records have been used.

Whether the data is coming from a tag or Android Beam the result is always an incoming Intent. The data from the Intent can be retrieved with the method *getParcelableArrayExtra*. An example of how to read a message and get its records is shown in Code Snippet 7. (AndroidDevelopers, NFC Basics) (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)

```
Parcelable[] rawMsgs = intent.getParcelableArrayExtra(  
    NfcAdapter.EXTRA_NDEF_MESSAGES);  
NdefMessage msg = (NdefMessage) rawMsgs[0];  
NdefRecord[] ndef_recs = msg.getRecords();  
String nfcData_firstRecod = new String(ndef_recs[0].getPayload());
```

*Code Snippet 7: read NDEFMessage (AndroidDevelopers, NFC Basics)*

We can differ between two approaches to enable the receiving of NDEF messages:

- enableForegroundDispatch
- enableReaderMode

### 5.2.4.1 *enableForegroundDispatch*

To make sure that a foreground Activity will get priority to handle a discovered tag the method *enableForegroundDispatch* can be used.

The Intent Filter in the manifest file is used to register for specific events if the app is not started. But if the application is already in foreground we don't want the launcher to get started. The foreground Activity should handle the incoming Intent without interruption. In order to do this an Intent Filter needs to be defined. It is recommended to do this in the Activities *onCreate* method.

*The method* enableForegroundDispatch is used to set up the Intent Filter. The definition is normally done in the onResume method of the Activity and needs to be disabled before the Activities onPause callback finishes. After enabling the foreground dispatch an incoming beam or discovered tag will be delivered to the method onNewIntent where it can be handled. An example of how to define the Intent Filter, enable, and disable the ForegroundDispatch is shown in Code Snippet 8. (developer.android, kein Datum) (Chen, 2011)

```
@Override
protected void onCreate(Bundle savedInstanceState){
    ...
    //define a generic Intent
    mNfcPendingIntent = PendingIntent.getActivity(this, 0,
        new Intent(this,
            getClass()).addFlags(Intent.FLAG_ACTIVITY_SINGLE_TOP),0);

    // define an IntentFilter for action NDEF_DISCOVERED
    // with the mime type text/plain.
    IntentFilter ndefDetected = new
        IntentFilter(NfcAdapter.ACTION_NDEF_DISCOVERED);
    try {
        ndefDetected.addDataTypes("text/plain");
    } catch (MalformedMimeTypeException e) {}
    mNdefExchangeFilters = new IntentFilter[] { ndefDetected };
    ...
}

@Override
protected void onResume() {
    super.onResume();
    //setting up the IntentFilter defined in onCreate to filter for
    //incoming intents with the action NDEF_DISCOVERED
    //4 parameter = techList (is only used if the filter is set to
    //ACTION_TECH_DISCOVERED)
    mNfcAdppter.enableForegroundDispatch(this, mNfcPendingIntent,
        mNdefExchangeFilters, null);
}

@Override
protected void onPause() {
    super.onPause();
    nfcAdpt.disableForegroundDispatch(this);
}
}
```

*Code Snippet 8: defining an IntentFilter, enabling, and disabling the foregroundDispatch in an Activity*

#### 5.2.4.2 *enableReaderMode*

In Android 4.4 the method `enableReaderMode` was introduced. When using this mode in an Activity the NFC controller is restricted to Reader/Writer mode, meaning the Peer-To-Peer mode and Card-Emulation mode are disabled. This mode is normally used in combination with the Host-based Card-Emulation mode where one devices acts as card and another one as reader. In opposition to `enableForegroundDispatch` a `ReaderCallback` needs to be defined in order to handle a discovered tag. Code Snippet 9 gives an example regarding the usage of `enableReaderMode`. (AndroidDevelopers, `enableReaderMode`)

```

//setting up the readerFlags. Looking for NFC tags of type A (including Android devices)
and preventing the check for NDEF-formatted data (e.g. Android Beam)
public static int READER_FLAGS = NfcAdapter.FLAG_READER_NFC_A |
NfcAdapter.FLAG_READER_SKIP_NDEF_CHECK;

@Override
public void onCreate(Bundle savedInstanceState){
    ...
    mNfcAdapter.enableReaderMode(this, new NfcAdapter.ReaderCallback(){
        @Override
        public void onTagDiscovered(Tag tag){
            //handle discovered tag
        }
    }, READER_FLAGS, null);
    ...
}

```

*Code Snippet 9: enableReaderMode example*

## 5.2.5 Writing NDEF message to tag or sending over beam

We can distinguish between writing data to a tag and sending data over Android-Beam to another device. The principle is the same. The data that should be written is defined as a NDEF message. The processing starts automatically when a tag is discovered. The example in Code Snippet 10 shows how to define a NDEF message with two plain text records.

```

NdefRecord[] ndefRecords= new NdefRecord[2];
ndefRecord[0] = createRecord("Hallo NFC");
ndefRecord[1] = createRecord("second Record");
NdefMessage message = new NdefMessage(ndefRecords);

public NdefRecord createRecord(String text) throws
    UnsupportedEncodingException
{
    String lang      = "en";
    byte[] textBytes = text.getBytes();
    byte[] langBytes = lang.getBytes("US-ASCII");
    int    langLength = langBytes.length;
    int    textLength = textBytes.length;
    byte[] payload    = new byte[1 + langLength + textLength];

    // set status byte (see NDEF spec for actual bits)
    payload[0] = (byte) langLength;

    // copy langbytes and textbytes into payload
    System.arraycopy(langBytes, 0, payload, 1,          langLength);
    System.arraycopy(textBytes, 0, payload, 1 + langLength, textLength);

    NdefRecord recordNFC = new NdefRecord(NdefRecord.TNF_WELL_KNOWN,
        NdefRecord.RTD_TEXT, new byte[0], payload);

    return recordNFC;
}

```

*Code Snippet 10: Creating a plain text NDEF message (Codexpedia)*

### 5.2.5.1 Writing to a Tag

Writing to a tag is similar to reading. To make sure that the foreground Activity gets priority for handling a detected tag `enableForegroundDispatch` should be used again. Code Snippet 11 shows how to write the message from Code Snippet 10 to a tag.

```
@Override
protected void onNewIntent(Intent intent){
    Tag mytag = intent.getParcelableExtra(NFCAdapter.EXTRA_TAG);
    //Get an instance of Ndef for the tag
    Ndef ndef = Ndef.get(tag);
    //Enable I/O operations
    ndef.connect();
    //Write message
    ndef.writeNdefMessage(message);
    //Close the connection
    ndef.close();
}
```

Code Snippet 11: Writing to a tag (Codexpedia)

### 5.2.5.2 Beaming NDEF Message

In order to use Android Beam to send a message from one device to another over Peer-To-Peer two different methods can be used (`AndroidDevelopers`, `setNdefPushMessage`, `setNdefPushMessageCallback`):

- *setNdefPushMessage*
  - When two devices are close enough the NDEF message from device A is automatically sent to device B.
- *setNdefPushMessageCallback*
  - In order to use this approach a callback containing the method *createNdefMessage* needs to be defined.
  - When two devices are close enough *createNdefMessage* is called.
  - The advantage is that if *createNdefMessage* returns null as message no beam will happen and the message is not static which gives a better control over the data exchange.

In order to be able to beam correctly (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013):

- both devices need to be unlocked
- the beaming Activity must be in foreground
- the data needs to be encapsulated in an NDEF message (see above)



Whether using *setNdefPushMessage* or *setNdefPushMessageCallback*, it is recommended to define both methods in the Activities *onCreate* method as shown in Code Snippet 12. Only one message can be sent during a beam. If both methods are registered the callback will get priority. (AndroidDevelopers, *setNdefPushMessage*, *setNdefPushMessageCallback*)

```
@Override
protected void onCreate(Bundle savedInstanceState){
    ndefMessage = new NdefMessage(ndef_records);
    //when a second device is in read range the method createNdefMessage
    // will be called - the actual content of ndefMessage will be sent
    mNfcAdapter.setNdefPushMessageCallback(nfcMessageCallback,this);

    //every time a second device is in read range the message will be sent
    //- the message that has been registered is static - does not matter
    //if it has changed in meantime
    mNfcAdapter.setNdefPushMessage(ndefMessageForSecondPlayer, this);
}
private NfcAdapter.CreateNdefMessageCallback nfcMessageCallback = new
NfcAdapter.CreateNdefMessageCallback()
{
    @Override
    public NdefMessage createNdefMessage (NfcEvent event){
        try {
            return ndefMessageForSecondPlayer;
        }
        catch(Exception e) {
            return null;
        }
    }
};
```

*Code Snippet 12: sending data over Android Beam with setNdefPushMessageCallback and setNdefPushMessage*

## 5.2.6 Host Card Emulation (HCE)

A Service is a component in Android that is used for long-running operations in the background. Services do not have a user interface but an Activity can interact with them. A typical use case for a Service would be to play background music for example. (AndroidDevelopers, Services)

A HCE Service is used for NFC applications working in Card Emulation mode. When a NFC card or a device working in Card Emulation mode is tapped to a reader, the communication starts.

Android devices can emulate cards based on NFC-Forum ISO-DEP specification since version 4.4 without involving a secure element. The ability to do so brings many new use cases. Any Android device can now be used instead of a smart card. Another advantage resulting from this is that bi-directional communication over NFC works now. In order to be able to make exchanges the card needs to be registered for the same Application ID (AID) the reader is looking for.

The basis of a HCE service in Android is the class *HostApuService*. It is based on the NFC Forum ISO-DEP protocol. Code Snippet 13 shows how to define a *HostApuService* in the Android Manifest. (AndroidDevelopers, Host-based Card Emulation)

```
<service android:name=".MyHostApuService" android:exported="true"
    android:permission="android.permission.BIND_NFC_SERVICE">
    <intent-filter>
        <action android:name="android.nfc.cardemulation.action.HOST_APDU_SERVICE"/>
    </intent-filter>
    <meta-data android:name="android.nfc.cardemulation.host_apdu_service"
        android:resource="@xml/aid_list"/>
</service>
```

*Code Snippet 13: defining a HostApuService for card emulation mode in “NFCQuiz”*

The meta-data tag is used to define the name of the xml-file that is containing the AID group declaration(s). An AID may consist of up to 16 bytes. AIDs for payment sector are well-known and public. Sometimes a HCE service needs to register multiple AIDs – in such cases an AID group is used.

The first byte is used to define the category of the AID. It is recommended to use the following rules for the AID-definition (ISO/IEC 2. , 2005):

- Internationally registered AIDs start with an “A”
- Nationally registered AIDs start with an “D”
- AIDs without registration start with an “F”

In case of “NFCQuiz” only one unregistered AID was needed. An example of the aid\_list.xml file can be seen in Code Snippet 14.

```
<host-apdu-service xmlns:android="http://schemas.android.com/apk/res/android"
    android:requireDeviceUnlock="false">
    <aid-group android:description="NFCQuiz AID"
        android:category="other">
        <aid-filter android:name="F111115555"/>
    </aid-group>
</host-apdu-service>
```

*Code Snippet 14: declaring AID for HCE service*

The communication unit between a reader and a card is called Application Protocol Data Unit (APDU). The specification for APDUs is defined in ISO/IEC 7816-4 (ISO/IEC, 2005).

One process in an application protocol can be defined as (CardWerk):

- sending data from the reader to the card
- processing the received data
- sending a response back to the reader

A command-APDU is sent by the reader. It consists of a mandatory head of 4 byte and an optional body of variable length. The card answers with a response-APDU consisting of an optional body and 2 mandatory status bytes at the end. (CardWerk)

The sequence diagram in Figure 40 gives a short overview of the connection process between reader and card.

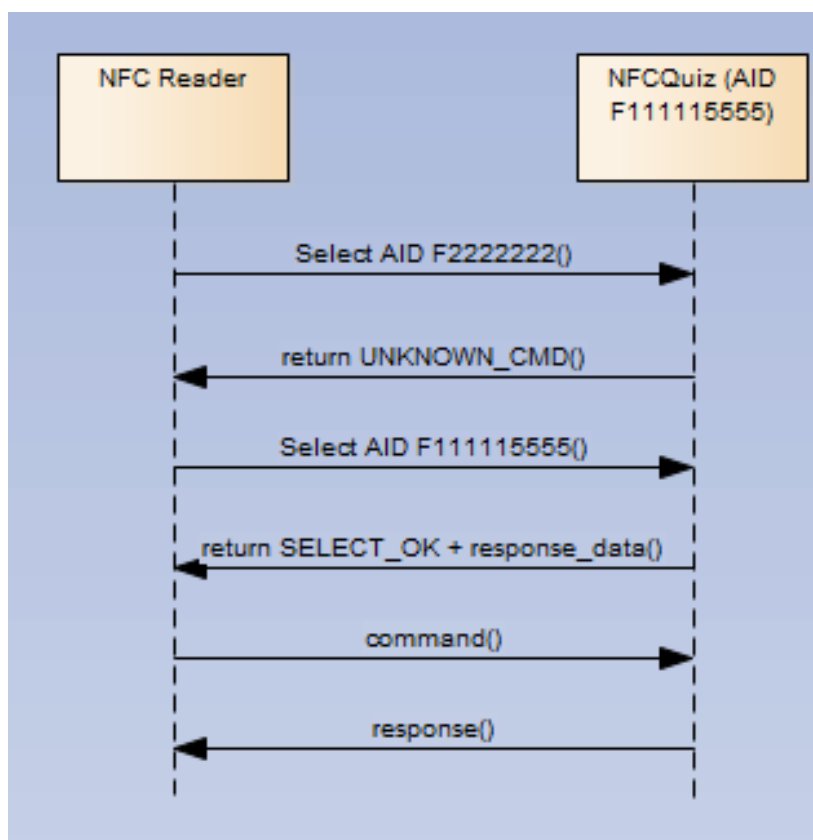


Figure 40: connection reader and card in card emulation mode

### 5.2.6.1 CardReader

The CardReader uses the *enableReaderMode* in order to disable all other modes beside the Reader/Writer mode. Since Android HCE uses the ISO-DEP protocol an IsoDep object needs to be acquired from the tag in order to get access to IsoDep properties and I/O operations (AndroidDevelopers, IsoDep). Only if the discovered tag supports the IsoDep interface a connection can be established and the reader can start looking for a matching AID on the (emulated) card. If a corresponding AID can be found the exchange between reader and card starts.

Code Snippet 15 gives an example of how to establish a connection, send and receive commands.

```

private static final String NFCQuiz_AID= "F111115555";
// "OK" status word sent in response to SELECT AID command (0x9000)
private static final byte[] SELECT_OK_SW = {(byte) 0x90, (byte) 0x00};
@Override
public void onTagDiscovered(Tag tag) {
    // Android's Host-based Card Emulation (HCE) feature implements the
    //ISO-DEP (ISO 14443-4) protocol. In order to communicate with a
    //device using HCE, the discovered tag should be processed using the
    //IsoDep class.
    IsoDep isoDep = IsoDep.get(tag);
    if (isoDep != null && !tagDiscovered) {
        try {
            // Connect to the remote NFC device
            isoDep.connect();
            isoDep.setTimeout(1000);
            // Build SELECT AID command for the service.This command tells the
            //remote device which service we wish to communicate with.
            byte[] command = BuildSelectAid(NFCQuiz_AID);
            // Send command to remote device
            byte[] result = isoDep.transceive(command);
            // If AID is successfully selected, 0x9000 is returned as the
            // status word (last 2 bytes of the result) by convention.
            //Everything before the status word is optional payload
            int resultLength = result.length;
            byte[] statusWord = {result[resultLength-2], result[resultLength-1]};
            if (Arrays.equals(SELECT_OK_SW, statusWord)) {
                tagDiscovered=true;
                byte[] payload = Arrays.copyOf(result, result.length - 2);
                //get the response data of the NFC device
                String response = new String(payload, "UTF-8");
                //send new message to the hce-device
                if(message!="") {
                    byte[] resultMessage = isoDep.transceive(message.getBytes());
                    message = "";
                    ...}
            }catch (IOException e) {}
        }
    }
}

```

Code Snippet 15: establishing connection with card, sending commands and receiving answers<sup>12</sup>

### 5.2.6.2 Host Card Emulation Service

The basis of a HCE service is the class `HostApuService`. It comes with two methods (`AndroidDevelopers`, Host-based Card Emulation):

- `byte[] processCommandAid(byte[] aid, Bundle extras)`
  - This method is called when a reader sends a command APDU to the service.
  - After sending the command the reader waits for a response APDU by the service.
  - An example is shown in Code Snippet 16
- `void onDeactivated (int reason)`
  - This method is called when the connection between reader and service breaks.

<sup>12</sup><https://github.com/googleamples/android-CardReader/blob/master/Application/src/main/java/com/example/android/cardreader/LoyaltyCardReader.java>

```
@Override
public byte[] processCommandApdu(byte[] commandApdu, Bundle extras) {
    byte[] return_value = UNKNOWN_CMD_SW;
    if(isRunning) {
        //get the payload
        byte[] payload = Arrays.copyOf(commandApdu, commandApdu.length);
        String command = "";
        try {
            command = new String(payload, "UTF-8");
        } catch (UnsupportedEncodingException ex) {}
        //check if the incoming command is the select APDU with the matching
        //AID
        if (Arrays.equals(SELECT_APDU, commandApdu)) {
            return_value = SELECT_OK_SW;
            //retrun the responseMessage + the OK Statusword
            if(responseMessage!="")
                return_value = ConcatArrays(responseMessage.getBytes(),
                    SELECT_OK_SW);
        }
        else
            return_value = UNKNOWN_CMD_SW;
        return return_value;
    }
}
```

*Code Snippet 16: get reader command and send response APDU after processing*

## 5.3 NFCQuiz guidance

The final game consists of two separate applications:

- NFCQuiz – the game itself
- NFCQuiz-Writer – an application that is used for writing the question-answer pairs to a tag

NFCQuiz is a multi-user quiz game. In the game we can distinguish between two roles:

- The *Reader*
  - reads the question set from a tag,
  - defines the final amount of players,
  - defines the amount of questions before synchronization.
  - The *Reader* can also be a *Card*. In this case we talk of an active *Reader*.
- The *Card*
  - receives the questions from the *Reader* over Android Beam.
  - The *Card* answers the questions and sends his/her statistics to the Reader by use of the Card Emulation mode.

The game settings are made by the user who is taking the part of the *Reader*. The *Reader* imports a NDEF message consisting of one or more NDEF records from a NFC tag. Each record is representing one question with 3 possible answers and an identifier marking the correct answer. After successful import the *Reader* sends the NDEF message with additional settings to every contributing player over Android Beam. In order to get a game score and to be able to calculate the winner of the game synchronization between the players has to be done. Before the Reader starts the game he/she defines how often this synchronization needs to happen. Setting the synchronization number to 3 for example would mean: the contributing players (*Cards*) have to put their phones one after another to the *Readers* phone after every third question. Since synchronization between all contributing players would increase dramatically the more players are involved, the adjustment is done just with the Reader. Consequently the game score is only shown on the *Readers* phone if more than two players are involved in the game.

In the following chapters, the implementation of the two applications is described. The structure, operation, and the data exchange are explained in order to get a better understanding of the game. Finally, possible use cases for NFCQuiz are illustrated in Chapter 5.3.3.

### 5.3.1 NFCQuiz

The class diagram in Figure 41 is an overview of the used classes in NFCQuiz. The game is separated into three activities:

- MainActivity
  - The MainActivity is the main entry point of the application.
  - The Config class is used to save the user defined game settings.
  - The creation of NDEF records and messages as well as the reading from a tag is implemented in the NDEFController class.
  
- GameReaderActivity
  - This Activity is called if the player is the *Reader*.
  - This Activity uses the method *enableReaderMode* to disable all other modes except the Reader/Writer mode.
  - The reader callback is implemented in the class CardReaderCallback.
  - CardReaderCallback
    - The *onTagDiscovered* method of this callback gets called if the phone of a *Card* is held near the *Readers* phone.
    - This class requests the game results of a *Card* by sending APDU commands.
    - If the game is played in two-player mode (1 *Card* and 1 active *Reader*) the class sends the *Readers* game results to the *Card* as well.
  
- GameEmulatorActivity
  - This Activity is called if the player is a *Card*
  - The Activity starts and stops the CardEmulatorService before and after the synchronization with the *Reader*.
  - CardEmulatorService
    - This class implements the HCU mode
    - It receives commands containing messages from the ReaderService and returns a byte[] containing the game results of the *Card*.
    - When the CardEmulatorService receives a message it is forwarded to the GameEmulatorActivity for further processing.

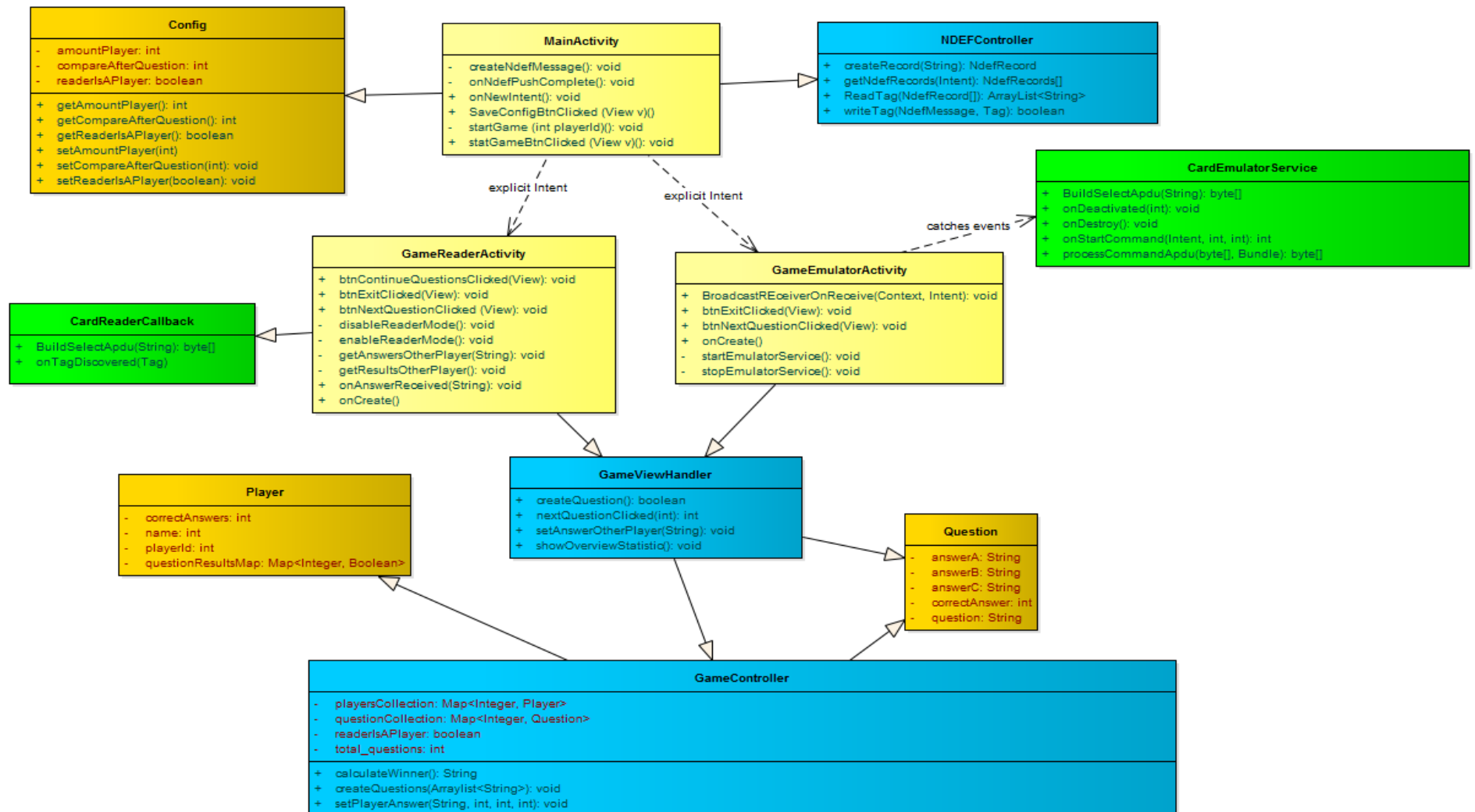


Figure 41: Class diagram of NFCQuiz application



### 5.3.1.1 *MainActivity*

The *MainActivity* consists of three layouts

- Main-layout
  - This layout is the starting point of the game.
  - As depicted in Figure 42 the layout consists of a name text field and three image buttons: Play, Cancel, and Settings
- Settings-layout
  - This layout is shown after the user presses the Settings button
  - An example of this layout is presented in Figure 43.
  - The layout is used by the *Reader* to define game-specific properties. Changes made by a *Card* will not be considered by the game.
- Progress-layout
  - This layout consists of a progress-bar and a text that prompts the user to initiate a NFC event (e.g. hold phone next to a tag in order to read the information on it).
  - Examples of the Progress-layout are depicted in Figure 44 and Figure 45.



Figure 42: Start layout (part of the MainActivity) showing the name text field, Start button, Cancel button, and Setting button



Figure 43: Setting layout (part of the MainActivity). The settings defined by the Reader will be used for the game.



Figure 44: TagReading layout (part of the MainActivity) requesting the Reader to hold his/her phone to the question tag and the Card to hold his/her phone to the Reader.

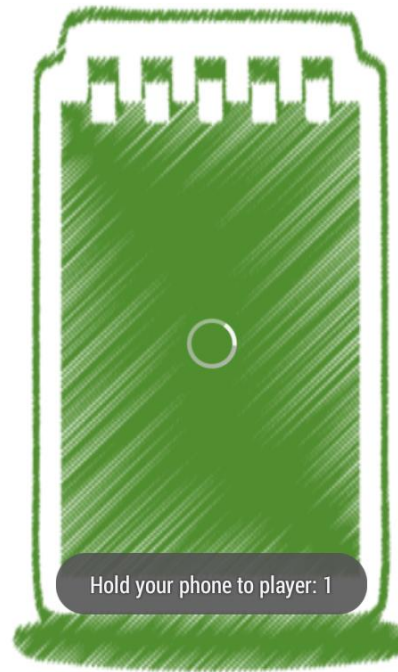


Figure 45: TagReading (part of the MainActivity) layout requesting the Reader to hold his/her phone to the first Card

At the beginning of the game the *Reader* enters the settings view and defines the following properties in the settings layout (Figure 43):

- the amount of contributing players,
- if he/she is one of the players,
- and if the synchronization with the players should happen after the last question or after a self-defined number of questions

Now the *Reader* goes back to the main menu and presses the Play button. The layout depicted in Figure 44 appears, telling the *Reader* to put his/her phone near the tag containing the question-answer pairs for the game.

The reading process is explained in Chapter 5.2.4. Once the reading is finished the layout shown in Figure 45 appears, requesting the *Reader* to put his/her phone to one of the *Cards* in order to transfer the questions set. This request is repeated for every contributing *Card*.

The NDEF message that is sent to the *Cards* is an extension of the message read from the tag. Every question-answer pair is saved in a NDEF record. The *Reader* extends the message with one additional record before beaming it to the *Cards*. The additional record contains the defined game settings and a consecutive *Card* ID. Every future message sent from a *Card* to the *Reader* contains this ID in order to be able to distinct the *Cards* from each other. As a result every *Card* gets a “personalized” message with the following content:

- the *Card* ID,
- if the *Reader* is a contributing player or not,
- the amount of questions before a comparison needs to be done with the *Reader*,
- the questions set

When a *Card* receives a NDEF message over Android Beam the *onNewIntent* method is called. The extraction of a NDEF message to string records is described in Chapter 5.2.4. This resulting string records are saved into an *ArrayList* and sent to the *Cards* *GameEmulatorActivity* over an explicit *Intent*. After all *Cards* have received the questions over Android Beam the *GameReaderActivity* is started for the *Reader*, again with an explicit *Intent* containing the tag questions in an *ArrayList*.

This process is depicted in Figure 46 for the *Reader* and in Figure 47 for the *Card*.

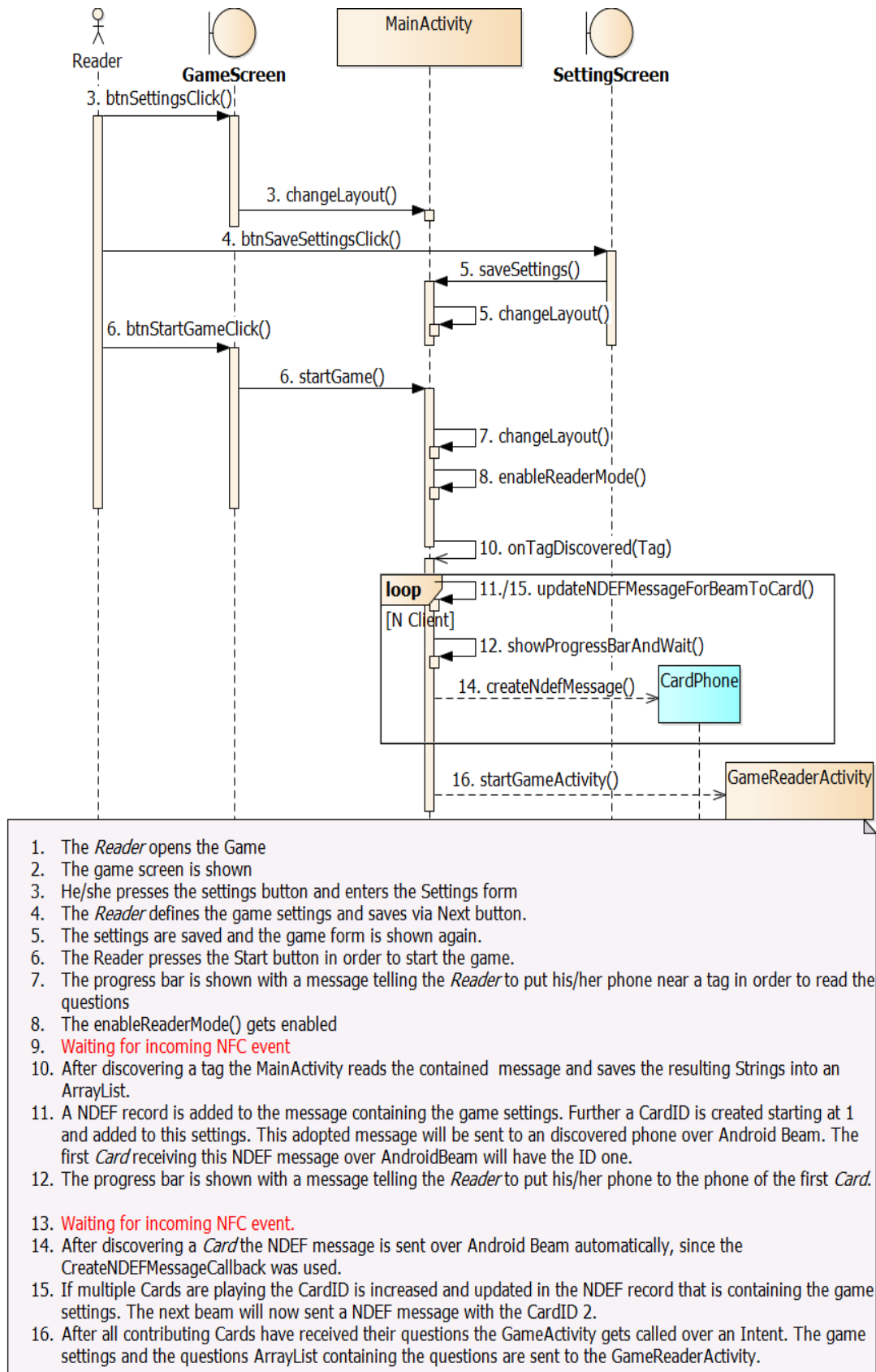


Figure 46: MainActivity sequence for Reader

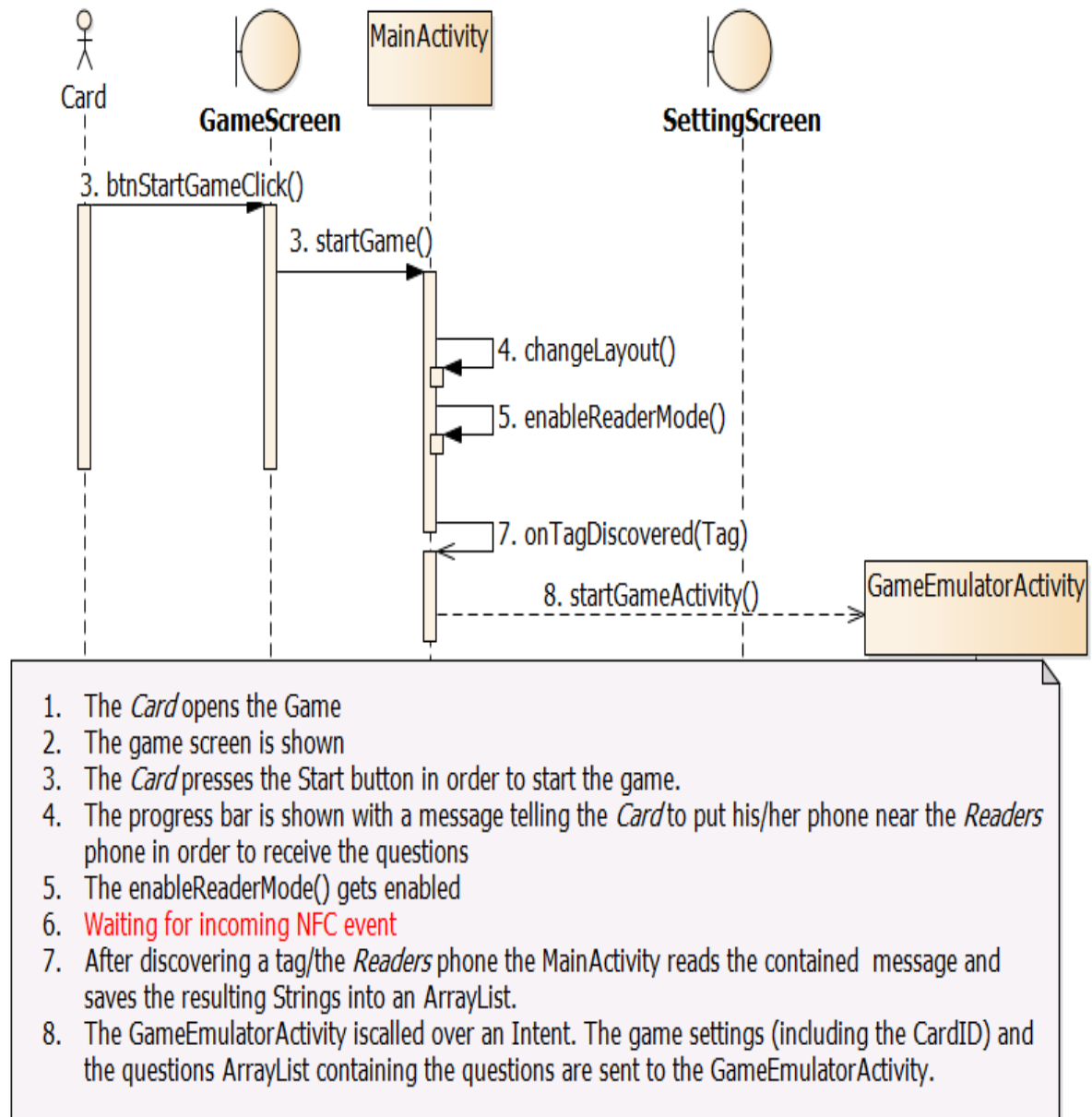


Figure 47: Main Activity sequence for Card

### 5.3.1.2 *GameReaderActivity and GameEmulatorActivity*

Even though the game layout is the same for both roles the handling in the background is different for the two roles. While the *Reader* operates in R/W mode the *Cards* are working in Card Emulation mode.

The extraction of the records to question objects is done in the *GameController* class. A detailed overview regarding the question-format is given in Chapter 5.3.2.1. After all records have been properly extracted the game starts. Figure 48 shows the game-layout. Each question is presented with 3 possible answers. By pressing the Next button a player confirms his/her answer. Depending on the amounts of questions the *Reader* has defined to be shown before synchronization, either the next question appears or a request telling the player to start the synchronization (shown in Figure 49). After each adjustment an overview-layout as depicted in Figure 50 is shown. A message can only be sent from one device to another. In order to get the game results of  $N$  players to all involved phones an exchange over NFC would need to be done  $\binom{N}{2}$  times. This would result in 10 exchanges for 5 players. Since the synchronization rate would raise dramatically with every additional player the overview-statistics are only calculated on the *Readers* phone if more than 2 players are involved.

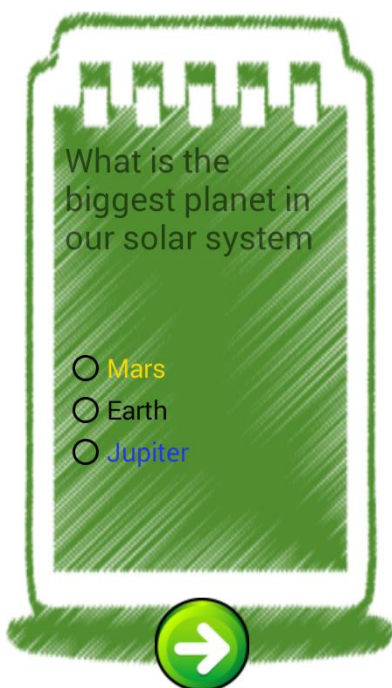


Figure 48: question layout (part of *GameActivity*) showing one question with 3 possible answers and a Next button

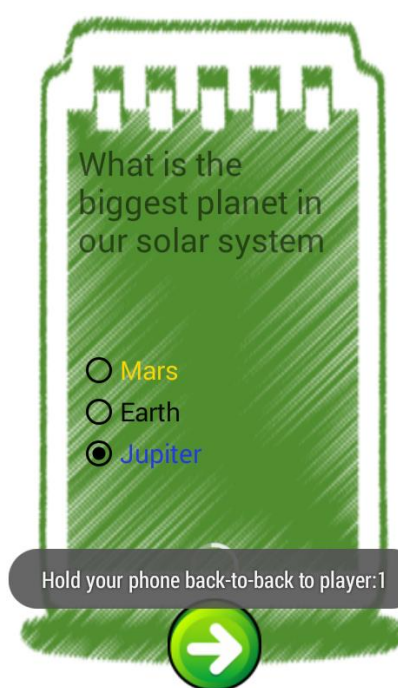


Figure 49: request telling the *Reader* to start synchronization with the first *Card*. If the prompt is addressed to a *Card*, the text will request him/her to put his/her phone back-to-back to the *Readers* phone.



As have already been mentioned the *Reader* works in R/W mode. When a tag is discovered in its read range a command, containing its AID and, if only 2 players are playing, the reader's results are sent to the tag.

A *Card* is emulating a card. When the *Card* presses the Next button the HCE service is activated waiting for an incoming command. After receiving the *Reader's* command APDU the *Card* answers with its question results and a status word indicating that everything was received correctly. A detail description regarding the code used for card reader and card emulator mode is given in the Chapter 5.2.6.2.

The overview layout is shown in Figure 50 and Figure 51. It provides a summary over the already answered question and the user answers. If all questions have been answered the game winner is calculated, otherwise the actual leading player is estimated (shown in Figure 51).

The GameActivity process is depicted in Figure 52 and in Figure 53 once for the Reader and once for the Card. Because of overview issues only the main actors are shown in the sequence diagrams.

Overview		
	Peter	Julia
Q1	✘	✔
Correct:	0	1

**Leading player: Julia**




Figure 50: Overview layout (part of GameActivity) showing a summary regarding the answered questions for every contributing player

Overview		
	Peter	Julia
Q1	✘	✔
Q2	✔	✘
Q3	✔	✘
Q4	✔	✘
Correct:	3	1

**Winner: Peter**






Figure 51: Overview layout (part of GameActivity) showing the final summary for all questions and the game winner.

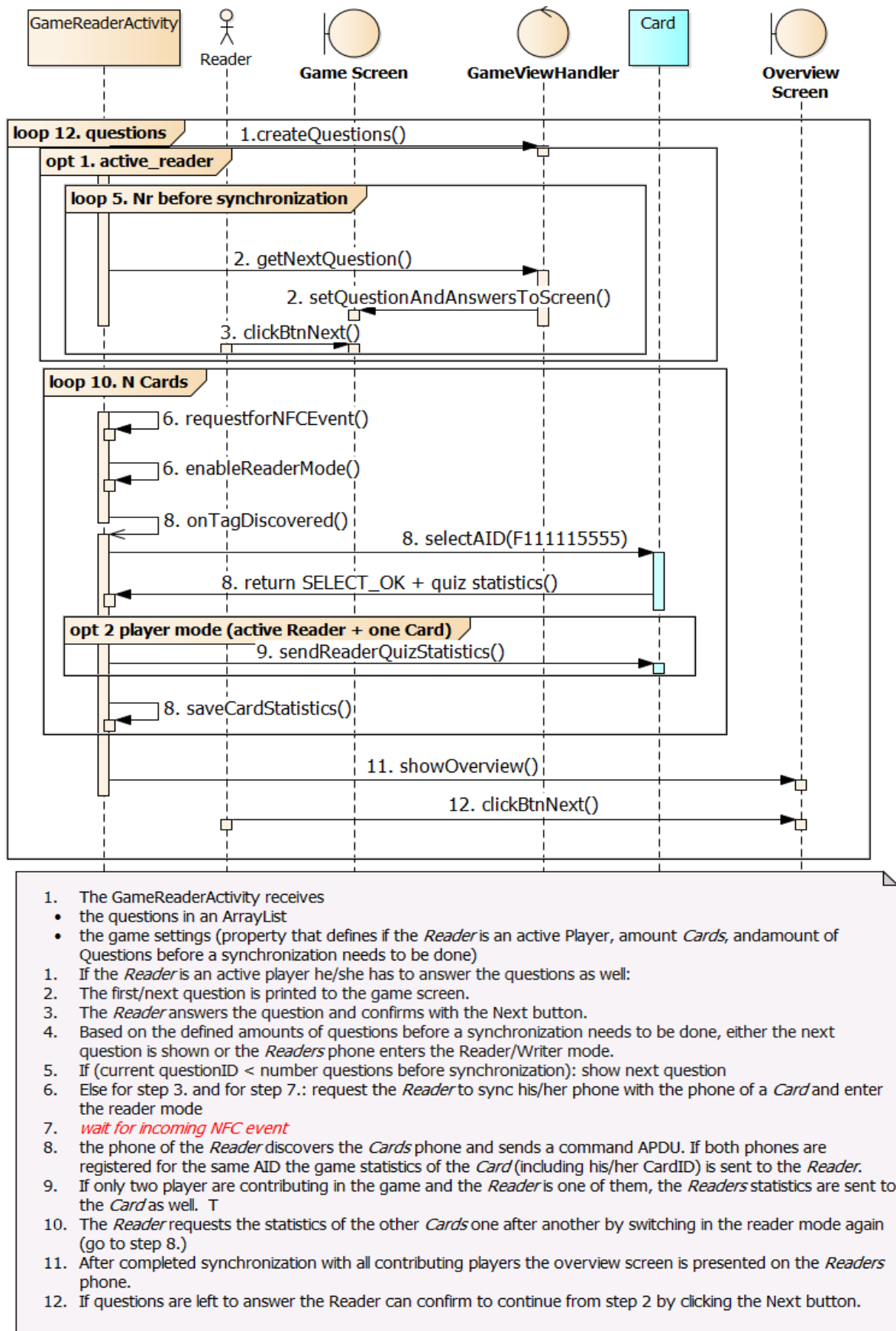


Figure 52: GameActivity sequence for a Reader



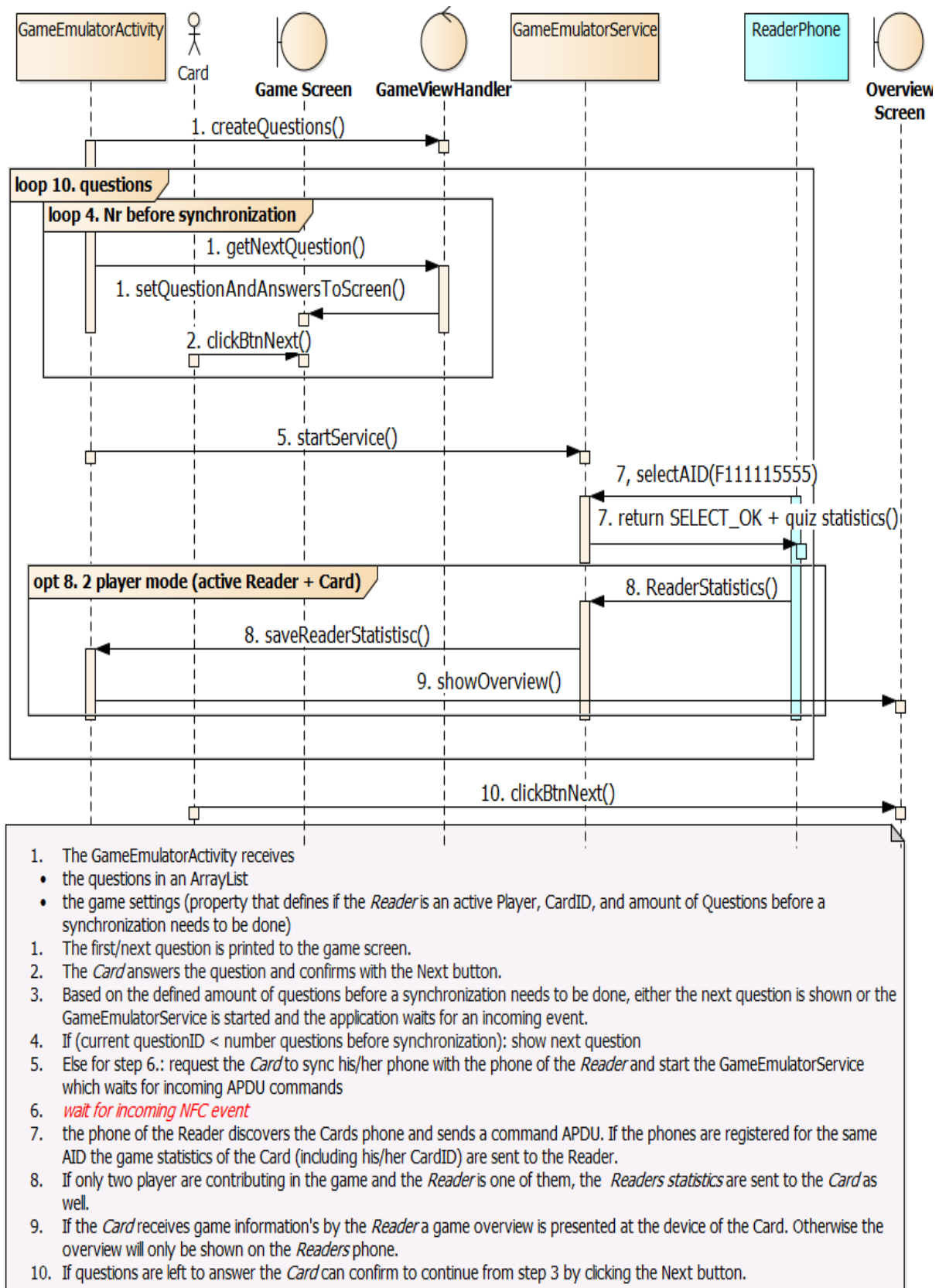


Figure 53: GameActivity sequence for a Card

## 5.3.2 NFCQuiz-Writer

This application has been created as it was not possible to find a free application that is able to write multiple NDEF text records to one tag. An alternative would have been to write one big message and to separate the question-answer-pairs by a special character. Nevertheless a solution with a user-specific layout seemed to be the best solution.

The NFCQuiz-Writer was separated from the NFCQuiz game because

- its functionalities are not exclusively bound to the game
- a separate app was considered as the idea is that the questions are written to a tag by a teacher/parent

### 5.3.2.1 Question-Format

The biggest problem about saving the questions to a tag is the available memory. For the application 4 different types of tags have been used:

- Topaz 512 sticker with 512 byte memory (NFC Forum Type 1 Tag)
- NTAG213 sticker with 144 byte memory (NFC Forum Type 2 Tag)
- DESFire EV1 keychain with 4096 byte memory (NFC Forum Type 2 Tag)
- NTAG216 smart card with 888 byte memory (NFC Forum Type 2 Tag)

One record (question and answers) needs per average about 80 byte memory. Considering this, the NTAG214 was not the right solution for the game. To use as little memory as possible plain/text record types have been used with the CSV format shown in Table 11.

1 record:	Question;answerA;answerB;answerC;correctAnswerId
2 record:	Question;answerA;answerB;answerC;correctAnswerId

Table 11: NFCQuiz question format

A corresponding example to this format is shown in Figure 54.

```
What is the biggest planet in our solar system;Mars;Earth;Jupiter;3
What is the chemical symbol for the element oxvgen:H:O:Ag:2
```

Figure 54: example of 2 question records in NFCQuiz

NFCQuiz-Writer supports 2 ways of writing a NDEF message to a tag:

- Upload over a CSV file
- Defining the question records in the user interface one by one

Every question-answer-pair is encapsulated into a NDEF record. The records are in turn part of a NDEF message. Chapter 5.2.5.1 describes how to create a NDEF message and write it to a discovered tag.

The Main screen of NFCQuiz-Writer is depicted in Figure 55. The tag writing can be done either by importing the questions set from an existing CSV file or by defining the questions one by one in the application.

- CSV file:  
In order to use this option the questions set needs to be defined in the format as described in Table 11. Otherwise NFCQuiz won't be able to separate the questions correctly. After pressing the CSV button in the main form a file chooser dialog appears where the user can select the CSV file containing the questions set.
- Defining questions in the application:  
The question-answer pairs can be defined one by one in NFCQuiz-Writer as well. The layout (Figure 58) is similar to the one used for NFCQuiz. The user defines a question and three possible answers, whereas the correct answer is identified through the radio button. An example of a defined question is depicted in Figure 59. The Plus button causes the creation of further questions. The Save button starts the writing process.

After choosing a CSV file or pressing the Save button the questions set is encapsulated into a NDEF message. The layout depicted in Figure 57 appears telling the user to put his/her phone near a tag in order to write the data. The *enableForegroundDispatch* method was used in order to be able to identify a tag and give priority to the NFCQuiz-Writer Activity. The writing process starts after a tag is discovered in read range as explained in Chapter 5.2.5.1.

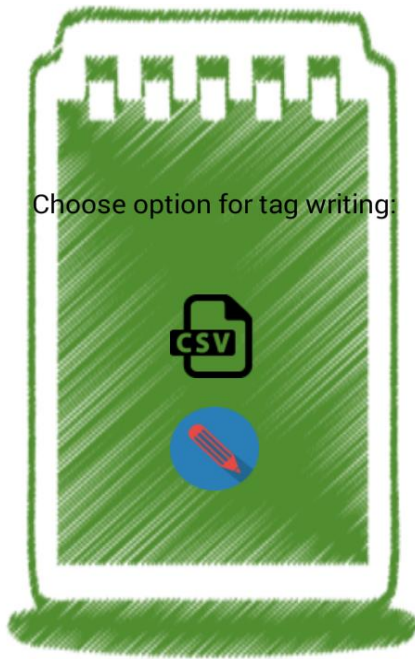


Figure 55: NFCQuiz-Writer main layout showing 2 buttons: Writing from CSV file and creating records in the app

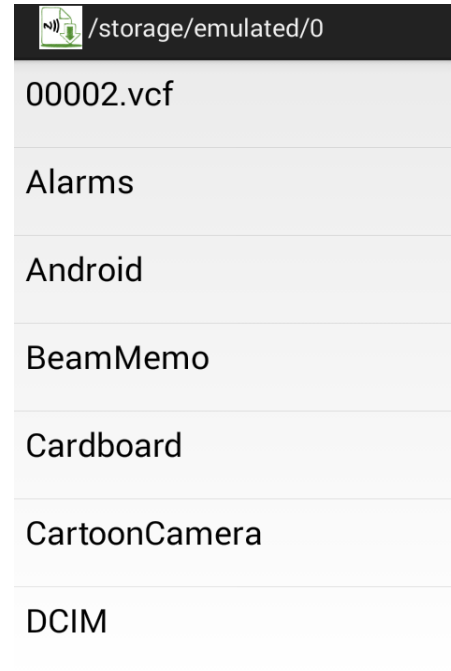


Figure 56: File chooser dialog of NFCQuiz-Writer. Shown after click on CSV button in the main screen.

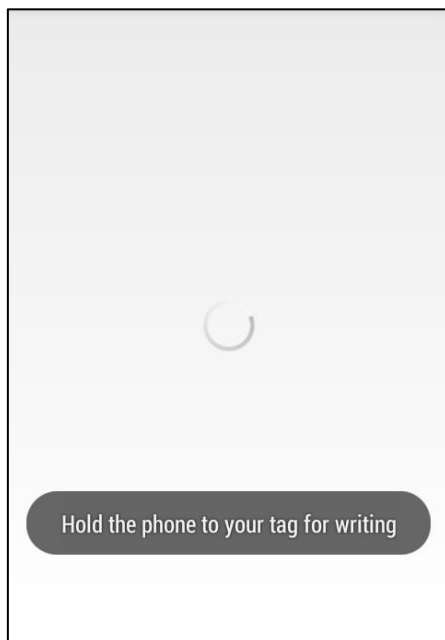


Figure 57: NFCQuiz-Writer – the progress bar layout appears if the application is waiting for an incoming NFC event

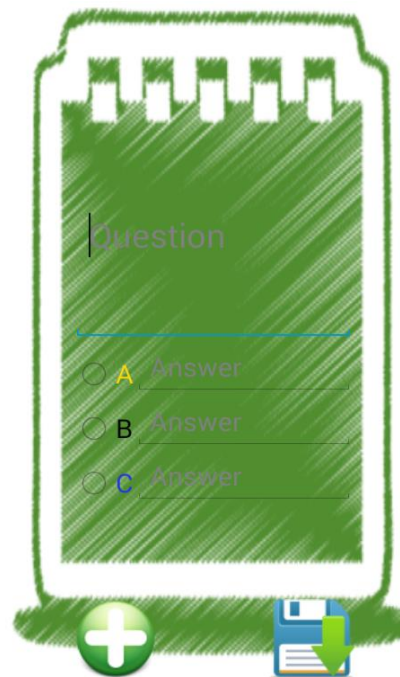


Figure 58: Create question layout in NFCQuiz-Writer

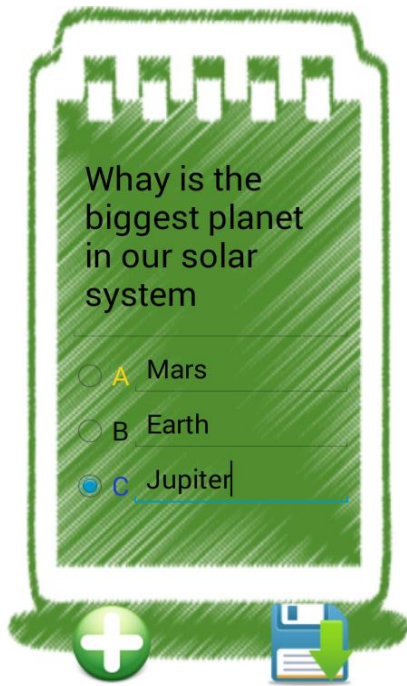


Figure 59: Create question layout in NFCQuiz-Writer with an example

### 5.3.3 Application examples

NFCQuiz is designed in a way that one *Reader* and one or more *Cards* need to contribute. Since a teacher/parent should have the opportunity to control the game and to adjust the questions/answers between all players without participating in answering of the questions the *Reader* doesn't need to be one of the contributing players.

The standard configuration of NFCQuiz is set up for 2 players where the *Reader* is an active player. Further the standard synchronization setting is set to be done after each question.

### *Example 1: Standard configuration with a predefined tag*

Suppose two kids playing NFCQuiz. The game starts equally for both players. The main screen is shown as depicted in Figure 42. Each player enters his/her name and presses the Play button.

In the next step the screen shown in Figure 44 appears telling each player to put his/her phone with its back either to the tag containing the questions or to the *Readers* phone. Since only two gamers are playing it does not matter who will read from the tag. One of the players, let's say player A, puts his/her phone to the tag in order to read all questions from it. Once the reading process is done player A is requested to hold his/her phone to the phone of player B in order to send the questions to him/her as well. After the transfer/receipt the game starts with the first question for both players equally.

Since the standard configuration is defined to make the synchronization after each question the form shown in Figure 49 appears each time a player presses the Next button. Players are not forced to answer questions within a special amount of time, so no time limit is imposed. An exchange can only be done if both players have answered their question and confirmed their answer with the Next button.

If the phones are close enough together the exchange of the game state is done in Card Emulation mode where one of the phones emulates a card and the other one a card reader. Once the exchange has finished, the actual game summary is presented to each player (example shown in Figure 50). The game continues after pressing the Next button in the overview form.

This process is repeated till all questions are answered. The final screen shows the game summary with the calculated winner below as depicted in Figure 51.

#### *5.3.3.1 Example 2: 2 Players and 1 passive Reader*

Suppose a parent with two children who wants them to repeat learned lessons with the help of NFCQuiz. In order to do so, the parent (=Reader) opens the NFCQuiz-Writer application, defines the questions-set, and writes it to a tag.

Now the *Reader* starts NFCQuiz game and opens the settings form. The configuration for this scenario would be:

- Amount Player: 2
- Comparison at the end
- TagReader is a player: unchecked

The *Reader* defines these settings and saves them by pressing the Next button in order to return to the main-screen. A click on the Start button triggers the form shown in Figure 44. Like in the first example the *Reader* needs to hold his/her phone to the tag in order to get all questions. After successful reading he/she will be requested to beam the questions-set in sequence to the contributing players (Figure 45).

Both children (A and B) start the game by entering their names and pressing the Start button. Now each of them needs to put his/her phone to the *Readers* phone in order to get the questions.

The game starts for A and B after correct receipt. Since the synchronization was defined to be done at the end, both players need to answer all questions till the request appears asking each of them to put his/her phone to the *Readers* phone. Suppose B has finished prior to A. B puts his/her smartphone to the *Reader* and transfers the game results. The *Reader* waits now till A finishes as well before creating a final game summary. The player order is irrelevant for synchronization. The overview screen containing an overall summary with the game winner is only presented on the *Readers* phone since only he/she has all player results.

### 5.3.3.2 Example 3: *N* Players and 1 active Reader

A possible scenario could be:

- A teacher defines the questions and answers prior by using NDEFQuiz-Writer
- He/she gives the resulting tag to a group of students
- One of the students takes the part of the *Reader* while he/she is a contributing player as well

Settings:

- Amount player: *N*
- Comparison after how many questions: *N*
- TagReader is a player: checked

The game scenario is the same as in example 2 with the following differences:

- the *Reader* needs to answer the questions as well
- The synchronization can only start after the *Reader* has answered the defined number of questions.

## 5.4 Discussion

This section is a reflection of the practical part. A deeper look into the potential of NFC for game based learning solutions should be given.

The presented application is just a prototype. The current version needs a tag with enough memory for the defined questions. Considering the fact that NFC tags do not come with great memory this could be handled by splitting the records into multiple messages distributed over more tags.

Possible scenarios when using NFCQuiz:

- Scenario1:
  - A teacher creates the questions multiple times on different tags and gives each tag a group of students.
  - In this scenario one student would be the *Reader* whereas the others would take the role of the *Cards*.
  - The settings for the game would be:
    - Amount Player: (*Reader* + *Cards*)
    - Checkbox “TagReader is a player” is enabled
- Scenario2:
  - A teacher takes the role of the *Reader*.
  - The teacher reads the tag and beams the questions to all students.
  - The teacher himself/herself is no contributing player
  - Settings:
    - Amount Player: Amount of students
    - Checkbox “TagReader is a player” is disabled
- Scenario3:
  - Due to the fact that the game can be used without an internet connection it is a good solution as “time killer” on a journey
  - Instead of giving their children a movie to watch, parents could write questions on a tag and give it to them for playing. The fact that the kids are learning during the game can be considered as a plus.

Nevertheless, a similar game could even work without a tag. A computer with a NFC reader/writer attached to it could take the role of the *Reader* and additionally create the questions without an extern tag. Instructions and an overview of the current game state could be printed on a separate monitor.

In this way basically every board game could be reproduced by an application using NFC.



The expected advantages would be:

- No need of internet access
  - An exception could be the download of new issues or game scenarios.
- An interactive effect is given to the participants by holding the phones together for synchronization. A participant does not have to “only” press buttons on the phone.
- Currently existing traditional games could be reproduced cheaper and without the use of resources like paper or plastic.

The usage of NFC for distributing or sharing files for student purposes is not a realistic scenario. Uploading the files to a cloud or just sending them per mail seems to be more comfortable for such use cases.

By using NFC tags, actions can be triggered on a smartphone as well. A possible scenario could be a tag at the entrance to a lecture. When a phone is held to the tag it could be switched in the silence mode. Even the whole internet access could be disabled by tapping a device to a tag. The app Trigger<sup>13</sup> for example, is a free available application that can be used to write actions on a tag.

NFC is not the all-round solution for every problem. But dealing with this technology is for sure not wrong. The presented scenarios should be though-provoking. They are off course not covering all aspects in the usage of NFC.

---

<sup>13</sup> <https://play.google.com/store/apps/details?id=com.jwsoft.nfcactionlauncher&hl=de>

## 6 Summary and Conclusion

This master thesis has dealt with the subject contactless communication technologies. The greatest attention was devoted to the technology Near Field Communication in Chapter 3 and special in the Chapter 5 since it was the main component in the practical part.

Since NFC can be seen as an outcome of RFID this technology was introduced in Chapter 2 as some kind of entry to the topic. Chapter 4 is dedicated to other contactless technologies (e.g. QR Code, Barcode, Smart Cards) and especially the potential of NFC regarding their use cases.

The practical part of the work was described in Chapter 5. A prototype using NFC in the field of game based learning was introduced. Especially the implementation of the three NFC modes has been discussed in detail since it is still hard to find a comprehensive summary on this topic. Based on the experience in the practical part, I believe that this technology fits very well in the field of game development.

The conclusion result regarding the use of NFC was that the technology is still far away from its true potential. Especially the Card Emulation mode is a field that brings enormous possibilities in different use cases since it eliminates the disadvantage that no real communication between two devices could take place before.

Examples in Chapter 4 have shown that NFC can be used as a replacement for current contactless technologies. With the exception of Smart Cards, I do not believe that this will happen in practice. The replacement of Smart Cards by NFC has already started. Due to the researches in NFC my personal opinion is that NFC will overrun Smart Cards in a few years in the application field of entrance and payment system.

The big advantage of NFC is the fact that it can be used in addition to current technologies. Nevertheless, I think NFC will have to find its own application area as well. The presented prototype is a good example of what is possible beside the payment sector.



## 7 Bibliography

- adafruit. (n.d.). *adafruit*. Retrieved August 1, 2016, from <https://www.adafruit.com/product/364>
- Adaptalift. (2012, May 01). *Adaptalift*. Retrieved June 14, 2016, from [http://www.aalhysterforklifts.com.au/index.php/about/blog-post/rfid\\_vs\\_barcode\\_advantages\\_and\\_disadvantages\\_comparison](http://www.aalhysterforklifts.com.au/index.php/about/blog-post/rfid_vs_barcode_advantages_and_disadvantages_comparison)
- adweek. (2013, 4 30). *adweek*. Retrieved 2 2, 2016, from [adweek.com: http://www.adweek.com/adfreak/budweisers-buddy-cup-might-be-dumbest-high-tech-brand-innovation-yet-149048](http://www.adweek.com/adfreak/budweisers-buddy-cup-might-be-dumbest-high-tech-brand-innovation-yet-149048)
- Aguirre, J. I. (2007, February). *EPCglobal: A Universal Standard*. Retrieved August 15, 2016, from <http://web.mit.edu/smadnick/www/wp/2007-01.pdf>
- Ahson, S. A., & Ilyas, M. (2008). *RFID Handbook: Applications, Technology, Security, and Privacy*. CRC Press.
- Aikaterini Mitrokotsa, M. R. (n.d.). Classification of RFID Attacks. Amsterdam: Department of Computer Science, Vrije Universiteit. Retrieved August 01, 2016, from <http://www.cs.vu.nl/~ast/Publications/Papers/iwrt-2008.pdf>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved August 25, 2016, from <https://developer.android.com/guide/components/intents-filters.html>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 29, 2016, from <https://developer.android.com/guide/topics/manifest/intent-filter-element.html>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 31, 2016, from [https://developer.android.com/reference/android/nfc/NfcAdapter.html#setNdefPushMessage\(android.nfc.NdefMessage, android.app.Activity, android.app.Activity...\)](https://developer.android.com/reference/android/nfc/NfcAdapter.html#setNdefPushMessage(android.nfc.NdefMessage, android.app.Activity, android.app.Activity...))
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 29, 2016, from <https://developer.android.com/guide/components/services.html>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 29, 2016, from <https://developer.android.com/guide/topics/connectivity/nfc/hce.html>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 31, 2016, from <https://developer.android.com/reference/android/nfc/tech/IsoDep.html>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 25, 2016, from <https://developer.android.com/studio/intro/index.html>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 25, 2016, from <https://developer.android.com/guide/topics/manifest/manifest-intro.html>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 29, 2016, from <https://developer.android.com/guide/topics/connectivity/nfc/nfc.html>

- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved June 14, 2016, from <https://developer.android.com/reference/android/nfc/NfcAdapter.html>
- AndroidDevelopers. (n.d.). *Android Developers*. Retrieved July 29, 2016, from [https://developer.android.com/reference/android/nfc/NfcAdapter.html#enableReaderMode\(android.app.Activity, android.nfc.NfcAdapter.ReaderCallback, int, android.os.Bundle\)](https://developer.android.com/reference/android/nfc/NfcAdapter.html#enableReaderMode(android.app.Activity, android.nfc.NfcAdapter.ReaderCallback, int, android.os.Bundle))
- BarcodesInc. (n.d.). *Barcodes Inc.* Retrieved June 14, 2016, from <https://www.barcodesinc.com/faq/#what>
- Bhasker, R. (2001). *Bar Codes - Technology and Implementation*. Tata McGraw-Hill.
- Boden, R. (2016, January 27). *NFC World*. Retrieved August 30, 2016, from <http://www.nfcworld.com/2016/01/27/341707/us-emv-shipments-to-hit-617m-units-in-2016/>
- CardWerk. (n.d.). *CardWerk*. Retrieved August 25, 2016, from [http://www.cardwerk.com/smartcards/smartcard\\_standard\\_ISO7816-4\\_5\\_basic\\_organizations.aspx](http://www.cardwerk.com/smartcards/smartcard_standard_ISO7816-4_5_basic_organizations.aspx)
- Castro, L., & Wamba, S. F. (2007, March). AN INSIDE LOOK AT RFID TECHNOLOGY. *Journal of Technology Management & Innovation*, pp. 128-141.
- Chen, J. (2011, August 30). *jessechen.net*. Retrieved July 31, 2016, from <http://www.jessechen.net/blog/how-to-nfc-on-the-android-platform/>
- Codexpedia, 2. (n.d.). *codexpedia.com*. Retrieved July 31, 2016, from <http://www.codexpedia.com/android/android-nfc-read-and-write-example/>
- Corporation, I. T. (2007). *Intermec*. (I. T. Corporation, Editor, & Intermec Technologies Corporation) Retrieved 2015, from [http://www.intermec.com/public-files/white-papers/en/UHFvs.HF\\_RFID\\_wp.pdf](http://www.intermec.com/public-files/white-papers/en/UHFvs.HF_RFID_wp.pdf)
- Coskun, V., Ok, K., & Ozdenizci, B. (2011). *Near Field Communication (NFC): From Theory to Practice*. John Wiley & Sons.
- Coskun, V., Ok, K., & Ozdenizci, B. (2013). *Professional NFC Application Development for Android*. John Wiley & Sons.
- DeMers, J. (2014, April 30). *SearchEngineJournal*. Retrieved June 14, 2016, from <https://www.searchenginejournal.com/use-qr-codes-marketing-campaign/103049/>
- developer.android. (n.d.). *developer.android*. Retrieved July 31, 2016, from [https://developer.android.com/reference/android/nfc/NfcAdapter.html#enableForegroundDispatch\(android.app.Activity, android.app.PendingIntent, android.content.IntentFilter\[\], java.lang.String\[\]\)](https://developer.android.com/reference/android/nfc/NfcAdapter.html#enableForegroundDispatch(android.app.Activity, android.app.PendingIntent, android.content.IntentFilter[], java.lang.String[]))
- Dobkin, D. M. (2008). *The RF in RFIDD*. Elsevier B.V.

- EcmaInternational. (2013, June). Near Field Communication - Interface and Protocol (NFCIP-1). Retrieved January 18, 2016, from <http://www.ecma-international.org/publications/files/ECMA-ST/Ecma-340.pdf>
- EcmaInternational. (2013, June). Near Field Communication Interface and Protocol - 2 (NFCIP-2). Retrieved January 18, 2016, from <http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-352.pdf>
- Elliott, B. S. (2009). *Library.AutomationDirect.com*. Retrieved July 22, 2017, from <http://library.automationdirect.com/transformers-application-construction-and-efficiencies-issue-15-2009/>
- Ferrer, G., Dew, N., & Apte, U. (2010). When is RFID right for your service. *Int. J. Production Economics* 124, 414-425.
- Finkenzeller, K., & Müller, D. (2010). *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near Field-Communication*. John Wiley & Sons.
- Glover, B., & Bhatt, H. (2006). *RFID Essentials*. O'Reilly Media, Inc.
- Hunt, V. D., Puglia, A., & Puglia, M. (2007). *RFID: A Guide to Radio Frequency Identification*. Hoboken, New Jersey: John Wiley & Sons, Inc.
- Igoe, T., Coleman, D., & Jepson, B. (2014). *Beginning NFC*. O'Reilly Media.
- IHS. (2014, February 27). *IHS Markit*. Retrieved July 25, 2016, from <http://press.ihs.com/press-release/design-supply-chain/nfc-enabled-cellphone-shipments-soar-fourfold-next-five-years>
- ISO/IEC. (2005). ISO/IEC 7816-4. Retrieved August 25, 2016, from [http://www.embedx.com/pdfs/ISO\\_STD\\_7816/info\\_isoiec7816-4%7Bed2.0%7Den.pdf](http://www.embedx.com/pdfs/ISO_STD_7816/info_isoiec7816-4%7Bed2.0%7Den.pdf)
- ISO/IEC, 2. (2005). International Standard ISO/IEC 7816-4. (Second edition). Retrieved from [http://www.embedx.com/pdfs/ISO\\_STD\\_7816/info\\_isoiec7816-4%7Bed2.0%7Den.pdf](http://www.embedx.com/pdfs/ISO_STD_7816/info_isoiec7816-4%7Bed2.0%7Den.pdf)
- Jerry Banks, M. P. (2007). *RFID Applied*. Hoboken, New Jersey: John Wiley & Sons, Inc. .
- Karmakar, N. C. (2011). *Handbook of Smart Antennas for RFID Systems*. John Wiley & Sons.
- Karmakar, N. C., Koswatta, R., Kalansuriya, P., & E-Azim, R. (2013). *Chipless RFID Reader Architecture*. Artech House.
- Keen, I. (2009, April). NFC Technology Overview. Retrieved August 31, 2016, from <https://outlook.live.com/owa/?path=/attachmentlightbox>
- Kern, C. (2006). *Anwendung von RFID-Systemen*. Springer Science & Business Media.
- Kern, C. (2007). *Anwendung von RFID-Systemen*. Springer.

- Klair, D. K., Chin, K.-W., & Raad, R. (2010). <http://ro.uow.edu.au/>. Retrieved February 1, 2016, from <http://ro.uow.edu.au/cgi/viewcontent.cgi?article=2702&context=infopapers>
- Langer, J., & Roland, M. (2010). *Anwendung und Technik von Near Field Communication (NFC)*. Berlin Heidelberg: Springer.
- Liu, H.-C. (2016, February 1). <http://cdn.intechopen.com>. Retrieved from <http://cdn.intechopen.com/pdfs-wm/8475.pdf>
- Macias, E., & Wyatt, J. (2014, April). *ti.com*. Retrieved August 20, 2016, from <http://www.ti.com/lit/an/sloa192/sloa192.pdf>
- Maierhuber, M. (2013). *Potentiale von NFC für Lehr- und Lernunterlagen*. Graz: Institut für Informationssysteme und Computer Medien, Technische Universität Graz.
- NearFieldCommunication.org. (n.d.). Retrieved January 1, 2016, from <http://www.nearfieldcommunication.org/history-nfc.html>
- Nearfieldcommunication. (n.d.). *Nearfieldcommunication*. Retrieved June 14, 2016, from <http://www.nearfieldcommunication.org/qr-codes.html>
- NearFieldCommunication.org. (n.d.). *nearfieldcommunication.org (Tag Types & Modes of Operation)*. Retrieved January 18, 2016, from <http://www.nearfieldcommunication.org/tag-types.html>
- NFCForum. (2006, July 24). NFC Record Type Definition (RTD) Technical Specification. Retrieved August 24, 2016, from [http://www.cardsys.dk/download/NFC\\_Docs/NFC%20Record%20Type%20Definition%20\(RTD\)%20Technical%20Specification.pdf](http://www.cardsys.dk/download/NFC_Docs/NFC%20Record%20Type%20Definition%20(RTD)%20Technical%20Specification.pdf)
- NFCForum. (n.d.). *NFC Forum*. Retrieved January 18, 2016, from <http://nfc-forum.org/about-us/our-members/>
- NFCForum. (n.d.). *NFC Forum*. Retrieved January 18, 2016, from [http://members.nfc-forum.org/specs/spec\\_list](http://members.nfc-forum.org/specs/spec_list)
- NFCForum. (n.d.). *NFC Forum*. Retrieved January 18, 2016, from <http://nfc-forum.org/what-is-nfc/what-it-does/>
- NFCForum. (n.d.). *NFC Forum*. Retrieved January 18, 2016, from <http://nfc-forum.org/our-work/specifications-and-application-documents/specifications/record-type-definition-technical-specifications/>
- NFCWorld. (2016, July 26). *NFCWorld*. Retrieved July 29, 2016, from <http://www.nfcworld.com/nfc-phones-list/>
- Preradovic, S., & Karmakar, N. C. (2012). *Multiresonator-Based Chipless RFID: Barcode of the Future*. Springer Science & Business Media.

- QRCodeStickers. (n.d.). *QRCodeStickers*. Retrieved June 14, 2016, from <http://www.qrcestickers.org/about-qr-codes/positive-negative-aspects-of-qr-codes.html>
- Qrky. (n.d.). *Qrky*. Retrieved June 14, 2016, from <http://getqrky.com/blog/why-nfc-won%E2%80%99t-kill-qr-codes/>
- Quirk, R., & Borello, S. (2005). RFID: rapid deployment and regulatory. *Venable LLP White Paper*.
- Rackley, S. (2007). *Wireless Networking Technology: From Principles to Successful Implementation*. Newnes.
- RaspberryPiFoundation. (n.d.). *raspberrypi*. Retrieved February 1, 2016, from [raspberrypi.org: https://www.raspberrypi.org/products/model-a/](https://www.raspberrypi.org/products/model-a/)
- RaspberryPiFoundation. (n.d.). *Raspberrypi.org*. Retrieved February 1, 2016, from [Raspberrypi.org: https://www.raspberrypi.org/products/](https://www.raspberrypi.org/products/)
- RFIDJournal. (2010, 9 8). *RFIDJournal*. Retrieved 2 2, 2016, from <http://www.rfidjournal.com/blogs/experts/entry?7853>
- RFIDJournal. (2011, 11 14). *RFID Journal*. Retrieved February 2, 2016, from <http://www.rfidjournal.com/blogs/experts/entry?8958>
- RFIDJournal. (2013, September 9). *RFID Journal*. Retrieved August 24, 2016, from <http://www.rfidjournal.com/blogs/experts/entry?10736>
- RFIDJournal. (n.d.). *RFID Journal*. Retrieved August 24, 2016, from <http://www.rfidjournal.com/glossary/term?80>
- RFIDJournal. (n.d.). *RFID Journal*. Retrieved August 24, 2016, from <http://www.rfidjournal.com/site/faqs#Anchor-What-30408>
- Richardson, M., & Wallace, S. (2014). *Getting Started with Raspberry Pi: Electronic Projects with Python, Scratch, and Linux*. Maker Media, Inc.
- Rosistem. (n.d.). *ROSISTEM - Build your business*. (ROSISTEM) Retrieved June 14, 2016, from <http://www.barcode.ro/tutorials/barcodes/history.html>
- Sarac, A., Absi, N., & Dauzere-Peres, S. (2010). A literature review on the impact of RFID technologies on supply chain management. *Int. J. Production Economics* 128, 77-95.
- Segan, S. (2012, February 13). *PCMag*. Retrieved July 25, 2016, from <http://uk.pcmag.com/smartphones/66443/news/new-ti-chip-could-spread-nfc-in-smartphones>
- Shah, J. (2009). *Supply Chain Managemetn: Text and Cases*. Dorling Kindsley (India) Pvt. Ltd.
- Shu-qin, G., Wu-chen, W., Li-gang, H., & Wang, Z. (2010). Anti-collision Algorithms for Multi-Tag RFID. In C. Turcu (Ed.), *Radio Frequency Identification Fundamentals and Applications Bringing Research to Practice*. InTech.



- SmartCardAlliance. (2012, September 27). *Smart Card Alliance*. Retrieved January 18, 2016, from [http://www.smartcardalliance.org/resources/webinars/nfc\\_app\\_ecosystem/20120927\\_NFC\\_Application\\_Ecosystems.pdf](http://www.smartcardalliance.org/resources/webinars/nfc_app_ecosystem/20120927_NFC_Application_Ecosystems.pdf)
- Sower, V., Bellah, J., Zelbst, P., & Green, K. (2013, September 22). *RFID Journal*. Retrieved July 22, 2016, from <http://www.rfidjournal.com/articles/view?11008>
- Tajima, M. (2007). Strategic value of RFID in supply chain management. *Journal of Purchasing & Supply Management* 13, 261-273.
- Tamm, G., & Tribowski, C. (2010). *RFID: Informatik im Fokus*. Berlin Heidelberg: Springer.
- Thrasher, J. (2013, July 15). *RFID Insider*. Retrieved August 15, 2016, from <http://blog.atlasrfidstore.com/examples-of-rfid-nfc-marketing>
- Tiedemann, S. (n.d.). *nfcpy.readthedocs.org*. Retrieved January 18, 2016, from <http://nfcpy.readthedocs.org/en/latest/topics/snep.html>
- Unitag. (n.d.). *Unitag*. Retrieved June 14, 2016, from <https://www.unitag.io/qr-code/what-is-a-qr-code>
- Violino, B. (2005, Januar 16). *RFID Journal*. Retrieved August 8, 2016, from <http://www.rfidjournal.com/articles/view?1338>
- Violino, B. (2005, January 16). *RFID Journal*. Retrieved August 15, 2016, from <http://www.rfidjournal.com/articles/view?1337/>
- Violino, B. (2005, Januar 6). *RFID Journal*. Retrieved August 15, 2016, from <http://www.rfidjournal.com/articles/view?1337/3>
- Violino, B. (2005, Januar 16). *RFID Journal*. Retrieved 2015, from <http://www.rfidjournal.com/articles/view?1338>
- Violino, B. (2015, January 16). *RFID Journal*. Retrieved August 15, 2016, from <http://www.rfidjournal.com/articles/view?1339/>
- Want, R. (2006). An Introduction to RFID technology. *Pervasive Computing, IEEE*, pp. 25-33.
- WEBSCAN. (n.d.). *WEBSCAN - Barcode Verifiers*. Retrieved June 14, 2016, from <http://www.webscaninc.com/qr-code-introduction/>
- Weightman, G. (2015, September 23). *Smithsonian.com*. Retrieved June 14, 2016, from <http://www.smithsonianmag.com/innovation/history-bar-code-180956704/?no-ist>

## 8 List of Figures

Figure 1: EPC Global structure 96-bit version (Kern, Anwendung von RFID-Systemen, 2006)	13
Figure 2: RFID components (Tamm & Tribowski, 2010)	14
Figure 3: communication Reader and Tag	15
Figure 4: RFID Transponder	16
Figure 5: Transponder Classes (Tamm & Tribowski, 2010)	17
Figure 6: A key chain is a very popular example of a RFID-tag with a plastic housing. This type of tags typically comes with a larger memory.	19
Figure 7: LF glass tags are available in different sizes (12-32 mm). The main use case is the identification of animals	19
Figure 8: RFID smart cards are typically used for access control and the payment sector	19
Figure 9: RFID smart label can be found in many forms and sizes. This type of tag is very popular as an alternative to QR codes and barcodes	19
Figure 10: Amplitude change based on frequency	20
Figure 11: coupling types in RFID	22
Figure 12: Basic Transformer Components (Elliott, 2009)	22
Figure 13: Inductive coupled RFID system (Finkenzeller & Müller, 2010)	23
Figure 14: Electromagnetic Backscatter coupling (Finkenzeller & Müller, 2010)	24
Figure 15: RFID communication mode (Finkenzeller & Müller, 2010)	26
Figure 16: Master-slave principle RFID participants (Preradovic & Karmakar, 2012)	27
Figure 17: types of available RFID readers (Preradovic & Karmakar, 2012)	29
Figure 18: RFID reader with multiple tags in its read range, all tags try to transfer data to the reader at once	34
Figure 19: Anti-collision protocols overview (Klair, Chin, & Raad, 2010) (Langer & Roland, 2010)	35
Figure 20: Tree based anti-collision strategy (Shu-qin, Wu-chen, Li-gang, & Wang, 2010)	37
Figure 21: Possible Attacks RFID (Finkenzeller & Müller, 2010)	39
Figure 22: Animal transponder overview (Finkenzeller & Müller, 2010)	43
Figure 23: Buddweiser's buddy cup	44
Figure 24: NFC protocol specifications (Keen, 2009)	51
Figure 25: NDEF message structure (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)	54

Figure 26: Example Sign Record (Langer & Roland, 2010)..... 59

Figure 27: NFC P2P protocol stack (Langer & Roland, 2010) (SmartCardAlliance, 2012) ... 65

Figure 28: P2P communication between two active devices ..... 66

Figure 29: Principle of P2P communication (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013) ..... 66

Figure 30: NFC p2p mode (touch to share) ..... 68

Figure 31: Reader/Writer protocol stack (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013) ..... 70

Figure 32: Reader/Writer mode communication between an active and a passive component71

Figure 33: participants of reader/writer communication (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013)..... 71

Figure 34: Card Emulation protocol stack (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013) ..... 73

Figure 35: Card Emulation mode communication between an active and a passive component ..... 74

Figure 36: Card Emulation participants (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013) ..... 74

Figure 37: Summary regarding NFC properties..... 79

Figure 38: Example Barcode (© 1994 – 2016 Barcodes, Inc) ..... 81

Figure 39: Activity chooser sequence for discovered tag (AndroidDevelopers, NFC Basics) 97

Figure 40: connection reader and card in card emulation mode ..... 104

Figure 41: Class diagram of NFCQuiz application ..... 109

Figure 42: Start layout (part of the MainActivity) showing the name text field, start button, cancel button, and setting button..... 111

Figure 43: Setting layout (part of the MainActivity). The settings defined by the Reader will be used for the game..... 111

Figure 44: TagReading layout (part of the MainActivity) requesting the Reader to hold his/her phone to the question tag and the Card to hold his/her phone to the Reader. .... 111

Figure 45: TagReading layout requesting the Reader to hold his/her phone to the first Card111

Figure 46: MainActivity sequence for Reader ..... 113

Figure 47: Main Activity sequence for Card..... 114

Figure 48: question layout (part of GameActivity) showing one question with 3 possible answers and a Next button ..... 115

Figure 49: request telling the Reader to start the synchronization with the first Card. If the prompt is addressed to a Card, the text will request him/her to put his/her phone back-to-back to the Readers phone. .... 115

Figure 50: Overview layout (part of GameActivity) showing a summary regarding the answered questions for every contributing player..... 116

Figure 51: Overview layout (part of GameActivity) showing the final summary for all questions and the game winner. .... 116

Figure 52: GameActivity sequence for a Reader ..... 117

Figure 53: GameActivity sequence for a Card ..... 118

Figure 54: example of 2 question records in NFCQuiz ..... 119

Figure 56: NDEF-Writer main layout showing 2 buttons: Writing from CSV file and creating records in the app ..... 121

Figure 57: File chooser dialog of NDEF-writer. Shown after click on CSV button in the main screen..... 121

Figure 58: NFCQuiz-Writer – the progress bar layout appears if the application is waiting for an incoming NFC event..... 121

Figure 59: Create question layout in NDEF-Writer ..... 121

Figure 60: Create question layout in NDEF writer with an example ..... 122

## 9 List of Tables

Table 1: RFID frequency overview (Violino, What is RFID, 2015) (Corporation, 2007) (Ferrer, Dew, & Apte, 2010).....	25
Table 2: NFC forum members categories (NFCForum, Our Members).....	49
Table 3: NDEF record fields description (Langer & Roland, 2010) (adafruit) (Igoe, Coleman, & Jepson, 2014).....	56
Table 4: RTD types (Langer & Roland, 2010) (NFCForum, Record Type Definition Technical Specifications).....	58
Table 5: NDEF-Message example .....	60
Table 6: NFC Tag types (Langer & Roland, 2010) (Coskun, Ok, & Ozdenizci, Professional NFC Application Development for Android, 2013) .....	62
Table 7: Raspberry Pi models overview (RaspberryPiFoundation, raspberrypi) (RaspberryPiFoundation, Raspberrypi.org) .....	76
Table 8: Comparison between RFID, barcode and NFC for the use in tracking systems (Adaptalift, 2012).....	85
Table 9: comparison of QR-Code and NFC regarding the use for marketing issues (QRCodeStickers), (Qrky) .....	87
Table 10: RFID, NFC, QR Code, Barcode usability for different use cases.....	91
Table 11: NFCQuiz question format.....	119

## 10 List of Code Snippets

Code Snippet 1: set NFC permission in Android Manifest.....	94
Code Snippet 2: defining the minSDKVersion .....	95
Code Snippet 3: define NFC as needed hardware feature.....	95
Code Snippet 4: Android Manifest from NFCQuiz-Application. Intent-filter to define main-activity for app launcher.....	96
Code Snippet 5: defining an Intent-Filter with respect to an AAR on a discovered NDEF tag (AndroidDevelopers, NFC Basics, kein Datum).....	97
Code Snippet 7: retrieve NFC adapter .....	97
Code Snippet 8: read NDEFMessage (AndroidDevelopers, NFC Basics) .....	98
Code Snippet 8: defining an IntentFilter, enabling, and disabling the foregroundDispatch in an Activity.....	99
Code Snippet 10: enableReaderMode example.....	100
Code Snippet 11: Creating a plain text NDEF message (Codexpedia).....	100
Code Snippet 12: Writing to a tag (Codexpedia) .....	101
Code Snippet 12: sending data over Android Beam with setNdefPushMessageCallback and setNdefPushMessage.....	102
Code Snippet 14: defining a HostApuService for card emulation mode in “NFCQuiz” .....	103
Code Snippet 15: declaring AID for HCE service .....	103
Code Snippet 15: establishing connection with card, sending commands and receiving answers .....	105
Code Snippet 17: get reader command and send response APDU after processing .....	106