Near Field Communication in Smartphones

Simon Burkard
Master Student, Computer Engineering
Dep. of Telecommunication Systems, Service-centric Networking
Berlin Institute of Technology, Germany
Email: simon.burkard@campus.tu-berlin.de

Abstract—**Near Field Communication (NFC) is an emerging wireless short-range communication technology that is based on existing standards of the Radio Frequency Identification (RFID) infrastructure. In combination with NFC-capable smartphones it enables intuitive application scenarios for contactless transactions, in particular services for mobile payment and over-the-air ticketing. The intention of this paper is to describe basic characteristics and benefits of the underlaying technology, to classify modes of operation and to present various use cases. Both existing NFC applications and possible future scenarios will be analyzed in this context. Furthermore, security concerns, challenges and present conflicts will be discussed eventually.**

I. Introduction

Within the last couple of years an expansive process has begun to emerge integrating computational logic into various kinds of objects of our everyday life and allowing us to persistently interact with those object. The idea is to thoroughly connect virtual information to objects of the physical world and thus providing ubiquitous computing. Related to the concept of network ubiquity is the term 'Internet of Things' referring to objects of daily use being identifiable, trackable, and even virtually connected via an internet-like structure [1].

An essential enabler for this vision is the technology of Near Field Communication (NFC) that provides the possibility of linking virtual information between physical devices through proximity. Almost every object or place can be equipped with a NFC tag and thus provide proximate identification and useful related information to a nearby user of a smart device, like a tablet computer or a smartphone. A poster advertising a music concert (see Figure 1) could for example not only offer information about the event itself to a user who taps the poster with his device, but also allow him to buy a concert ticket dispensed directly to his phone. The interaction technology behind remains invisible to the user, being unobtrusively stuck to the object, i.e. the concert poster, whilst being available anytime. When entering the concert hall, the validity of the ticket can be approved by simply waving the smartphone across a NFC reader device at the entrance control. After having enjoyed the performance, the visitor could share photos he's taken during the concert with another visitor by simply holding their tow phones together. And - just to follow this scenario - when taking the bus home afterwards, the user is not required to tediously gather coins the get a bus ticket at the vendor machine. Instead, when entering and leaving the bus, he touches his phone to a reader device and the cheapest ticket price is automatically debited from his account. The presented scenario perfectly emphasizes possible key benefits of pervasive communication afforded by NFC technology: a larger degree of mobility and simplicity whilst decreasing the amount of physical effort required.

As pointed out, in most scenarios a smart device is essential for enabling ubiquitous computing with NFC technology. The smartphone market however is currently growing tremendously. According to a study of the International Data Corporation (IDC) a total amount of 118 million smartphone devices were sold worldwide during the third quarter of 2011, leading to an increase of 42.6% compared to the same period of time in 2010 [2]. In Western Europe in the second quarter of 2011 already, the shipment of smartphones has outranged feature phone shipments for the first time [3]. One can assume that sooner or later the majority of people will be in possession of a smart device and thus being able to deploy and use NFC based communication and interaction - subject to the condition that manufactures react in an adequate way and add NFC support to their devices.

The intention of this paper is to summarize opportunities provided by combining the technology of Near Field Communication with the capabilities of modern smartphones. It will point out recent trends and present application scenarios, but also address challenges and obstacles that might occur when trying to make NFC suitable for the mass market.

First, it will be necessary to provide a basic technical understanding of Near Field Communication. The first chapter will thus roughly explain the functionality of NFC and its underlying technique of Radio Frequency Identification (RFID). Its characteristics will be described and necessary hardware components and different modes of operation will be specified. The subsequent chapter will present NFC application case studies. It will cover both already existing applications as well as imaginable scenarios that are not available yet respectively tested only in trials. Main focus will lie on mobile payment appliances using the example of the lately released Google Wallet. Furthermore, examples for mobile ticketing will also be discussed as well as possible applications for medical assistance and for other market segments. The final part of this paper will deal with potential security issues and other challenges mostly related to present conflicts due to clashing interest of different groups of stakeholders. Addressing this topic is essential for eventually providing an outlook for the future development and estimation for the expected prospect of success in the context of Near Field Communication.

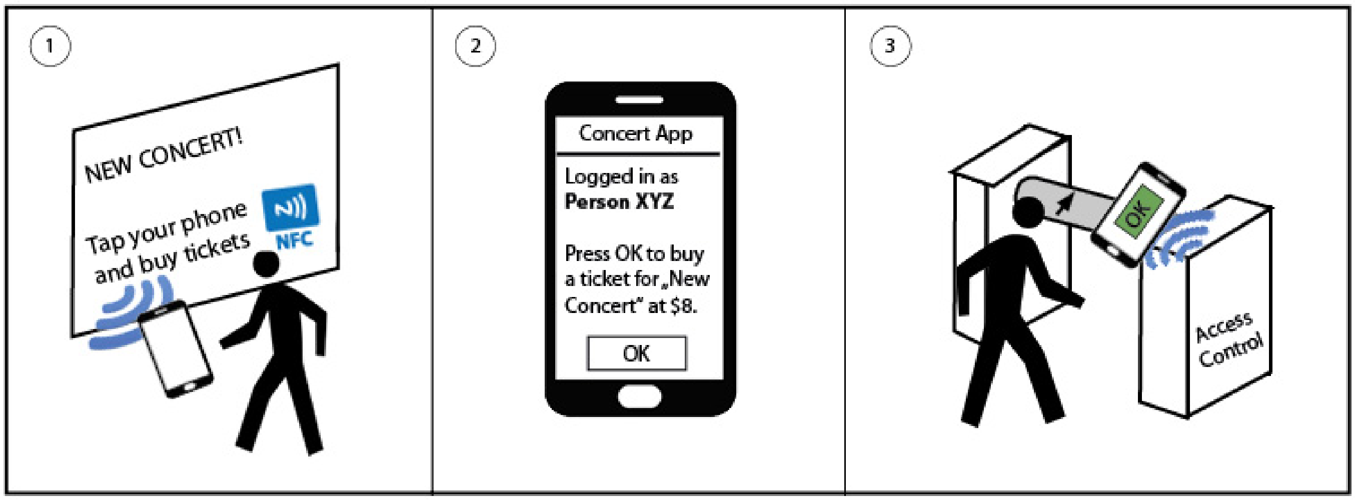
1
NEW CONCERT!
Tap your phone and buy tickets
NFC
2
Concert App
Logged in as Person XYZ
Press OK to buy a ticket for „New Concert" at $8.
OK
3
OK
Access Control

Fig. 1. A typical NFC application scenario: A user spots a smart poster advertising an upcoming concert and taps the poster with his NFC phone (1). A dedicated pre-installed application opens on his phone displaying details of the concert. As the user has already registered an account and is signed in, he is able to directly buy a ticket (2). The ticket is securely stored on his phone. Later, on site of the concert, the access control gates are equipped with a NFC reader and provide immediate access to the user (3).

II. NFC Technology

A. Technical Principles and Historical Progression

NFC is a short-range wireless communication technology that is based on approved and mature standards in the field of RFID and smart cards. RFID, which has already been introduced in the 1970s, realizes automatic identification and data transfer via electromagnetic radio signals typically my means of an active reader that is connected to a source of energy and a passive electronic tag that is a transponder receiving its power from the reader by magnetic induction. The RFID tag normally contains an antenna for receiving and transmitting the radio signal and an integrated circuit for processing and storing information and for modulating and demodulating the signal [4, pp13-26]. A usual tag is shown in Figure 2. The RFID tag can be placed almost everywhere and is normally hidden behind existing material, like the packaging of a product, thus being invisible to the user. Those passive RFID tags without own battery usually cost between $0.1 and $1 apiece. For many business models these costs of RFID tags are still relatively large resulting to the fact that until today RFID hasn't been integrated into daily use on this scale. Also, the lack of affordable and permanently available mobile devices containing RFID readers, has led to the more or less prevalent absence and unattractiveness of the RFID technology. [5]

In 2004, NXP Semiconductors, Sony and Nokia founded the NFC Forum in order to bring existing standards and efforts of the RFID and smart card technology together and to create a novel and innovative capability for short-range communication. Up to now, the NFC Forum counts more than 100 members and supporting companies aiming to find a worldwide standardization for the NFC technology [4, pp6-8]. For a long time, only a small handful of NFC mobile phones were available, mainly manufactured by Nokia, until Samsung and Google attracted a large audience when releasing the NFC supporting Nexus S phone in 2010. With the current rush on smartphones mentioned above and further successful NFC field tests in the past years, it is expected that in near future most of the top class smartphones will be equipped with NFC support [5].

B. Technical Characteristics and Operation Modes

One of the major advantages of NFC is the fact that the technology is compatible with existing RFID infrastructure, RFID tags and further contactless smart cards. NFC is built upon a subset of existing ISO standards, including the ISO/IEC 14443 standard that is being used by the RFID technology. NFC hence operates at the unlicensed 13.56 MHz radio frequency band with amplitude shift-keying modulation allowing transfer data rates up to 424 Kbits per second. Theoretically NFC works up to a distance of 20 cm, whereas in most scenarios a working distance of about four centimeters is usual. [4, pp87-91]

In contrast to conventional RFID systems, in the NFC technology there is no more strict distinction between reader and transponder. A NFC-capable device integrates both components: a passive transponder and an active reader. It can not only read and write data from or to a tag, but also receive and transmit data directly to another NFC device. Thus, NFC supports in overall three operating modes [4], [6, pp91-101]:

- *Reader/Writer mode*: The NFC capable device operates as an active reader or writer. As soon as it gets close enough to a passive RFID transponder tag or a passive smart card, energy is transferred to the passive tag via magnetic inductive coupling. After the tag being powered, a contactless communication can be established. The NFC device is then able to not only read information stored in the tag, but also to write data to the memory of the tag,

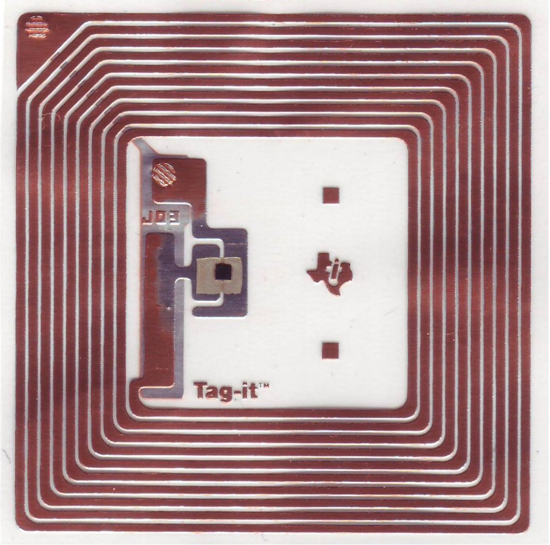

Fig. 2. A customary passive RFID tag that is compatible with NFC. A small microship is sourrounded by a copper antenna. The shown tag has a side length of around five centimeters. [7]

respectively the smart card. Typically such NFC tags can offer up to 4 Kbytes of memory.

- *Peer-to-Peer mode*: By simply holding two active NFC devices close together, this mode allows easy data exchange between the two devices.
- *Card Emulation mode*: In this mode the NFC device acts as a smart card so that other NFC devices can read data from it. This operation mode is used in particular for payment or ticketing applications or for providing access control. The NFC device thereby substitutes a credit card, paper-based ticket or an ID card, eventually leading to the elimination of the need for the accordant physical object.

C. NFC Data Exchange Format

In all modes of operation an NFC Data Exchange Format (NDEF) message is used for the transfer of data, no matter whether the communication takes places between two NFC devices or between one device and a passive NFC tag. The NFC Forum has hereby defined a universal set of rules for the data structures used for any kind of NFC communication. A NDEF message contains one or more NDEF records that each encapsulates user data of the application layer. The NDEF record is composed of a header and a payload part containing the actual user data. Apart from an ID that uniquely identifies the record, the header most notably defines the type and therefore of the format of the record data [4, pp120-122]. This could be either a MIME media type, describing a composition of e.g. images, textual content and any other types of information [4, p123], or one of the predefined NFC record type definitions (RTD). In contrast to the MIME media types, the latter specifications define not only the data structure, but also the way how the data should eventually be processed and presented on the receiving output device, i.e. the NFC handset. Amongst others, the following NFC record type definitions are possible:

- The *Text Record Type* allows the encapsulation of basic text strings including information about the character encoding scheme and the language of the text [4, p125].
- The *URI Record Type* contains a Uniform Resource Identifier, e.g. an email address or a web address. An application receiving this NFC record can for example be adjusted to automatically process this information to a web browser application [4, p126].
- The *Signature Record Type* offers a security mechanism by providing the possibility to sign a whole NDEF message. The application receiving the signed message can then verify its integrity and authenticity by cross checking the signature with a corresponding signature approved by a Certificate Authority [4, p133] [8]. The issue of NFC communication security will be addressed later in this paper in more detail.
- The *Smart Poster Record Type* provides a practical opportunity to augment physical objects, e.g. a smart advertisement poster equipped with a NFC tag, with the virtual content hence enabling the previously described concept of the ”Internet of Things’. The Smart Poster Type encapsulates multiple NDEF records containing for example a textual title record, a URI record and also a recommended action to perform when receiving that message, for example to open a certain URL with the browser or to compose a SMS message. Via a simple tap on the tagged object, a receiving NFC device can thus easily be provided with related content that is presented accordingly formatted [4, pp127-130]. In the scenario of buying a concert ticket, as shown in Figure 1, most probably such Smart Poster Record Type will be used.

D. Connection Handover

For the transfer of huge amounts of data at high speed or over a large distance between initiator and target the described capabilities of the NFC technology might not be sufficient. In theory however, NFC also provides a mechanism for a connection handover to an other wireless technology with higher data rates like Wi-Fi or Bluetooth. In general, the establishment of such data communication requires a lot of configuration effort. The simple touch-and-connect principle of NFC though can be used ideally in order to exchange the required configuration parameters. Following a technical specification provided by the NFC Forum in this way the negotiation sequence for activating a new communication channel can be achieved via NFC hence enabling an easy connection handover. [4, pp137-142] [5]

E. Hardware Architecture of NFC-capable Phones

Before presenting several NFC application scenarios in the subsequent chapter, it will be useful to discuss the basic NFC hardware components in smartphones and their role within the NFC communication flow. This will be useful to also understand the position and attitude of the various stakeholder parties and the resulting, later discussed, conflicts between them.

For NFC in mobile devices essentially four components are required: A Host Controller, a NFC Controller, a NFC Antenna and a Secure Element. [4, pp145-164]

The *Host Controller* acts as the heart of every mobile phone. This processor is not only necessary for executing the mobile's operating system, but also manages the user interface and the GSM/UMTS modem and serves as Application Execution Environment (AEE). It is the gateway for the other NFC components to the mobile phone's system itself and is therefore an essential part for integrating NFC functionality into the handset. The *NFC Antenna* obviously is needed for receiving and transmitting adequate radio signals. The *NFC Controller* modulates, demodulates and processes the signals in accordance with the mentioned NFC specifications whilst supporting all three modes of operation. Last but not least, the NFC architecture provides a *Secure Element (SE)* serving as Trusted Execution Environment (TEE). Many NFC systems deal with critical and sensitive data and therefore need a secure environment to store data and to execute applications being protected against manipulation and misuse. Such Secure Element can be integrated into a mobile phone in several ways. It could either be a dedicated chip that is a fixed part of the phones hardware or it could be realized as a removable and exchangeable chip card. Maybe the most evident and reasonably way is to use the Universal Integrated Circuit Card (UICC) as Secure Element. This card is provided by the mobile network operator (MNO) to its customers anyway and does not only contain the SIM module but also a multi-functional and secure platform for various applications. When switching to a new phone, the customer can hence easily continue to use his data applications stored on 'his' Secure Element, i.e. his UICC. However, the UICC is released by and bound to a specific network operator making it problematic to develop UICC based NFC applications without involving the MNOs. [9]

F. Comparison to Similar Technologies

Certainly, there are other technologies for wireless communication providing capabilities that are similar to the just presented RFID respectively NFC based specifications.

Bluetooth is a further short-range communication technology that can also be integrated into mobile phones. It operates at a higher frequency band of 2.4 GHz, provides greater data rates up to 2 Mbit/s and is therefore more suitable for the transfer of larger amounts of data. It allows considerably higher working ranges of several meters making it on the other hand easier to undesirably intercept signals. It hence provides less security. Furthermore, NFC connections can be established at once within a fraction of a second, whereas Bluetooth usually involves further configuration settings and user interaction or device pairing. However, a new Bluetooth feature, called Bluetooth low energy (BTE), also aims to provide a more usable, low-powered technology with much faster connection setup. [10]

Wi-Fi is another mechanism to exchange data wirelessly. It operates on the same frequencies as Bluetooth, but with higher power. This leads to more power consumption on the mobile device, but allows still higher data rates and larger working ranges of typically up to 100 meters. The connection setup is also quite complex and time consuming. Another important difference to NFC is the fact that both techniques, Wi-Fi and Bluetooth, are not able to communicate with passive, non-powered devices such as passive tags. [11]

QR codes provide capabilities that are similar to the usage of NFC tags. They represent two-dimensional optical barcodes, visualized by coded black and white patterns storing various types of data, i.e. up to several thousand characters depending on the tag's size and error correction level. Whilst generating virtually no costs, QR codes can be printed on different kinds of surfaces, typically on product packages and advertisement posters. In order to read the tag content, a camera sensor is required. In contrast to NFC tags they are thus not only more conspicuous, but also sensitive to the readers pose, lightning conditions and other disruptive conditions in the environment. QR tags are cheaper, but reading a QR tag with the built-in camera of a smartphone is in general more cumbersome and time consuming than reading a NFC tag. [5]

In some areas, NFC has certainly benefits compared to other technologies, but the comparison also reveals that those technologies can complement each other quite well. It is therefore likely that NFC will coexist with existing technologies like Wi-Fi and Bluetooth in future smartphones.

III. Applications

Near Field Communication offers great capabilities for various and comprehensive use cases. NFC applications can not only be built upon existing RFID infrastructure and therefore achieve cheap and fast acceptance and marketability, but also offer great usability. The technology is convenient, easy to use and intuitively familiar to people. They do not need to have any knowledge about the underlying technology as the communication starts automatically by simply bringing two devices, or a device and a tag respectively, physically together. Therefore, NFC is perfectly suited for mobile payment and ticketing scenarios. The presentation of such applications will hence be the main part of this chapter. In the end however, several other differing use case examples will also be mentioned.

A. Mobile Payment

Compared to traditional payment solutions, NFC payment primarily leads to faster and easier payment at the Point of Sale (POS), e.g. at the supermarket checkout or at a ticket vending machine. At present, a customer conventionally pays either by cash or with a debit card. In the first case when paying cash, the user is required to always carry cash money with him. Then, at the POS the proper amount of invoiced money as well as the change need to be counted and scrabbled together. This leads to a cumbersome and time-consuming procedure. Once an adequate payment terminal is available,

(a) The Wallet application is available for Android OS and compatible with MasterCard's PayPass NFC readers at shop checkouts. [12]

(b) Sensitive data is stored on a dedicated Secure Element within the phone. Before making a purchase, a PIN must be entered to access the data. [13]

Fig. 3. Google Wallet is one of the first mature NFC payment services, but still limited to a single smartphone model and to a sparse number of merchants.

paying with a usual debit card is certainly more efficient, but there is still an expenditure of time. The appropriate card needs to be picked out of the wallet, it needs to be inserted into the terminal with considering the correct orientation and the right PIN needs to be entered. With NFC payment a single movement of the hand is sufficient. By just waving the NFC-capable phone over the reader device, the payment is enforced. Entering a PIN however might still be necessary and advisable for security reasons. Moreover, the NFC phone can not only replace the debit card itself, but also store personalized discount coupons and bonus cards. This additionally contributes to making a traditional wallet becoming redundant. Also, a simple person-to-person money transfer is imaginable by simply holding two phones closely together and by using the discussed NFC peer-to-peer operating mode. On the user side, the biggest barrier however for using such contact-less ways of payment probably remains the psychological concern of feeling insecure when transferring sensitive data invisibly over the air without physical contact. Anyway, most of the major banks and related stakeholders have been working on trial applications and efficient architectures for NFC based mobile payment solutions.

1) Google Wallet: A first meaningful and promising concept available for the public has been developed by Google, called *Google Wallet* [12]–[14]. It was officially presented for the first time in May 2011 and launched in September 2011. Google Wallet is primarily built upon an application for Google's own operating system Android and is available at the Android market free of charge. Currently however, only a single NFC phone is supported, that is Google's Nexus S 4G smartphone. Also, the number of supported credit cards and the number of available payment locations is still limited at present. Google Wallet currently offers two types of payment instruments: owners of a Citi MasterCard credit card can directly link their banking account to Google Wallet. As of 2005 MasterCard has already begun to roll out a proprietary NFC based payment system called PayPass. This system originally was designed for credit cards with small built-in NFC chips, but now also serves as the basis for of the Google Wallet service infrastructure. So far, up to 300.000 merchant locations in the US are equipped with a MasterCard PayPass NFC reader likewise supporting Google Wallet [15] (see Figure 3(a)). In the meantime, another major credit card issuer has been jumped on Google's band wagon as Visa Inc. announced to make their similar PayWave infrastructure available to the Wallet service [16] . It is hence predictable that the availability of Google's payment service will soon grow rapidly, at least in the United States. At all supported merchant locations, customers who do not own a credit card of the eligible card issuers mentioned above are however also able to use the Google Wallet payment service. For this purpose Google provides a virtual Google Prepaid Card. This card can be funded by any credit card and its account is only available virtually in the NFC handset.

The Google Wallet does not only provide a payment card, but also can comprise and record personalized vouchers and loyalty cards by means of a service called Google Offers. Combined with other company-owned products like Google Maps and Google Places, this service offers deals e.g. on nearby vendors. Those discounts will be automatically redeemed when paying with Google Wallet on-site. The Google Offers service is furthermore a way for financing the Google Wallet application, which itself is free to use for both shoppers and merchants. By pushing sponsored offers to users of Google Wallet, Google is able to make money anyway.

This service of course has to deal with sensitive and personal data. The credit card information and credentials are therefore stored cryptographically secured in the Secure Element of the phone. For the Nexus S phone thereby a dedicated chip, named SmartMX, is used [17]. This chip is non-removable and seamlessly embedded in the handset while being completely separated from the usual phone's memory and operating system. This means that Google Wallet operates independently of the MNOs as not using their UICC module. Instead, it relies on the assistance of the handset manufactures that need to implement an applicable microchip as Secure

Element within their phones. This is presumably the reason why currently only one single phone, i.e. the Nexus S being subsidized by Google, is able to use the Wallet service. A 4-digit Wallet PIN additionally enhances the security of the payment process (see Figure 3(b)).

A typical payment scenario looks as follows: A Google Wallet user approaches an eligible merchant location and asks the cashier to pay via the Google Wallet service. The cashier enters the invoiced amount into his terminal and instructs the user to tap his phone on the NFC reader, e.g. a MasterCard PayPass reading device. Having done this, the Wallet application demands the user to enter his PIN before proceeding. Only now, when entering the correct PIN, the Secure Element chip and the NFC antenna is turned on. In order to perform the actual payment process, the user again taps the NFC terminal. The invoiced amount is virtually debited from the Wallet and the PayPass reading device eventually triggers the money transaction with the users bank account. As in this example the retailer also offers a certain bonus program, the Wallet application automatically earns some loyalty points giving some discount on the next purchase at this POS. On the smartphone and on the vendor's terminal a confirmation of the payment occurs and the user can leave the shop. A couple of minutes later, the NFC antenna and the SE chip on the user's handset are again disabled in order to avoid any security risks and to save battery power.

2) ISIS Consortium: The architecture most competing with Google Wallet is expected to be developed and provided by a consortium called ISIS. This consortium is mainly built upon a partnership between major players of the US mobile communication market including AT&T, T-Mobile and Verizon Wireless. Instead of building its own separate payment network infrastructure at the POSs, ISIS decided in May 2011 - due to financial reasons - to also run its service on existing payment networks like those run by Visa and MasterCard. By investing more than $100 million into the project and by entering a partnership with additional major credit card issuers like Discovery Card and BarclayCardUS, ISIS tries to successfully compete with Google on the NFC payment market. First pilot implementations are planned to be rolled out by ISIS in 2012. [18], [19]

3) SIMpass Technology: A different approach for mobile payment is conducted by a technique called SIMpass, developed and distributed by Watchdata System Ltd. This solution however is currently only available and adapted for the Chinese market. In cooperation with China Telecom the SIMpass technology is based on the following concept: an external NFC antenna that is manually placed between the battery and the back case of the mobile phone is connected to a special RFID-SIM card. This SIM card is put into the usual SIM slot of the phone providing normal SIM applications as well as contactless functions like payment services. By thus adding NFC support manually, this concept is completely independent of the handset architecture and is hence also applicable for phones that originally are not manufactured with NFC support. The payment process at the POS itself is however quite similar to the Google Wallet purchase scenario presented before. In China, SIMpass based contactless payment is already a commonly used technique. By March 2011, more than three million SIMpass units have been sold in China making this technology to the NFC payment system with the biggest user base so far. As being highly dependant on the MNO, this concept however is not supposed to become a worldwide success. [14], [20], [21]

4) P2P Payment: The payment solutions given so far all cover transactions between a single person owning a NFC capable phone and a vendor that is in possession of a NFC reader device. Furthermore, NFC offers the capabilities for simple peer-to-peer money transfer from person to person. In November 2011, PayPal released application offering such features for Android. PayPal's common business model is about easy payments between two users via the Internet. Therefore, a user, who is uniquely identified by his email address, links his PayPal account to a standard bank account or credit card. PayPal serving as a trusted third party is now able to exchange money between two users by simply debiting the first and crediting the second user's account. For NFC based P2P payment both users are required to have an account at PayPal and to install the mentioned application on their Android NFC phones. Via a ”Request Money” widget on the phone the payee enters the desired amount, bumps the phone of the second user and waits for a buzz to appear. The payer receives a notification on his phones immediately. After being confirmed by the user, the payment is then processed online via the PayPal servers. [22]

B. Mobile Ticketing

Beside mobile payment another large segment capable for NFC applications is mobile ticketing. In certain cases, both mobile ticketing and payment could even be combined into powerful and innovative appliances with great usability. Mostly in the field of public transport, extensive RFID infrastructure for ticketing and access control is already in use. The advantage of such systems essentially is to get rid of buying paper-based tickets at retail shops or ticket vendor machines. Instead, a RFID compatible smartcard is used to check the ticket validity and to debit the appropriate ticket price for each journey.

1) Oyster Card: One of the most popular systems for RFID based mobile ticketing is operating in London. The so-called *Oyster Card* works as contactless smartcard for prepaid mobile ticketing and can be used on all public transport services within the London area. All buses as well as entrance and departure gates of subway and train stations are equipped with RFID readers which the customers have touch with their Oyster cards when starting and ending their journey. Altogether more than 20.000 reading devices are installed in the field. In either case, the readers are able to read and write the cards in less than 300ms allowing a quick and straightforward access control and ticketing procedure. This form of system thus not only prevents travelers from using the transport systems without a valid ticket, but also can automatically debit the

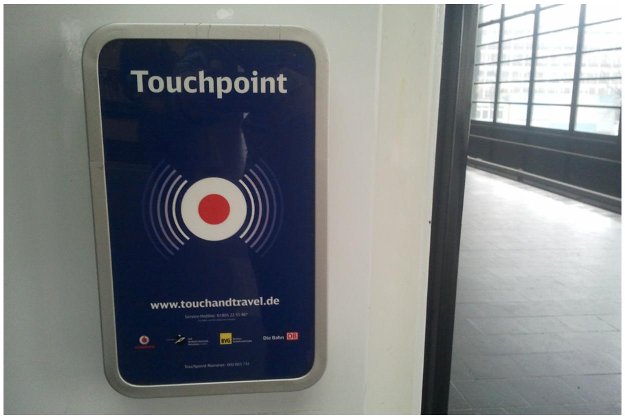

Fig. 4. A Touchpoint provides easy NFC ticketing to users of the Deutsche Bahn Touch&Travel service. The shown Touchpoint is located at the Berlin S-Bahn station 'Zoologischer Garten'.

Fig. 5. The Android Beam features is included in Android's newest version 'Ice Cream Sandwich' and allows data transfer between two NFC-capable smartphones. The figure shows two Samsung Galaxy Nexus phones exchanging a map location. [23]

appropriate fare from the card depending on the traveling type and duration. As a matter of course the card needs to be topped up in advance. This is usually done via cash or credit card at kiosks or at certain vending machines placed at the stations. Flat rate tickets, e.g. based on monthly subscriptions, can of course also be linked to the Oyster Card. As being technically compatible, this immense RFID based ticketing system can be extended for NFC support without much effort. This means that the smartcard could be replaced by a NFC enabled mobile phone. Tickets could be either bought online and disposed directly to the phone in advance or - combined with NFC payment - debited from a bank account automatically. After each journey the mobile handset could additionally display useful related information, e.g. the charged fare or the travel time, and hence provide further usability. In cooperation with Telefonica O2, Nokia, Barclaycard, Visa Europe and others, a six months trial for NFC based travel capabilities embedded in mobile phones has finished in 2008 with great success and positive user feedback. However, until now the London transportation system is still not working with NFC phones yet. Nevertheless, there are plans to deploy new contactless reading devices like the Visa PayWave or the MasterCard PayPass systems to Londons transportation network until 2013 thus allowing postpaid ticketing combined with NFC payment. [24]–[26] [4, p213]

2) DB Touch and Travel: In Germany, a similar system is gradually attracting attention. The project *"Touch and Travel"* run by Deutsche Bahn (DB) is also based on a best-price principle using check-in and check-out points at train stations which the users have to touch in order to trace their journey. For this purpose, so-called "Touchpoints" have been installed at the stations (see Figure 4). These are equipped with NFC tags storing location information. In order to use this system, customers are required to register their NFC phone and to install an application that is available for Android and iOS. At the beginning and end of their journey they tap the Touchpoint with their NFC phone. The place of location and hence the itinerary is determined and sent to Deutsche Bahn servers via the Internet. After checking out the cheapest price for the journey can be identified and at the end of the months the customer receives an invoice summing up all invoked activities. When being checked by ticket inspectors during the journey, a barcode on the mobile phone application verifies the ticket validity. As in German train stations there are no access control gates like in the London transport system, it is however rather difficult to check whether the user has checked in and out properly. Therefore, the application separately also tracks the users location in the background continuously, e.g. via GPS signals, and observes any inconsistencies. Due to the lack of NFC mobiles available at present in Germany, the Touchpoints also offer the opportunity to check in and out via scanning a QR code that is visible on each Touchpoint. The Deutsche Bahn Touch and Travel system thus currently also works with non-NFC capable mobile phones. [24] [4, p218]

3) Movie, Concert and Hotel Ticketing: The use of Near Field Communication does not only make sense for ticketing in public transport systems but also in various other areas that apply ticket reservation, ticket selling and admission control. In the introduction chapter an example for combining NFC with concert ticketing was already described: a user waves his NFC handset over a tagged advertisement poster and is redirected to a website where he can buy a ticket online. The ticket is cryptographically stored on the mobile phone and guarantees access on-site by being verified by a staff member with a NFC reading device or by an automatic entry barrier. The same procedure is applicable for movie tickets, conference entrance cards or hotel reservation. In the latter scenario NFC readers could for example be installed at the entrance of each hotel room. The NFC phones of the hotel guest could then operate as room keys providing access only to the booked rooms. [4, pp220-223]

C. Other NFC prototype applications

Possible applications that make use of the NFC technology are versatile and portable to almost every market segment.

Some useful prototyped applications will be described below.

1) Access Control: The already addressed access control mechanism is of course also eligible for personal admission controls in normal companies. At present, in many offices contactless RFID smartcards are used to identify staff members and to provide access into certain subareas of the company only to authorized persons. As a replacement for these smartcards, NFC capable smartphones could be used. The mobile phone is at hand anyway all the time for most employees. The costs for this changeover will be obviously quite low. [4, p224]

2) P2P Data Transfer: The P2P mode offered by NFC can certainly not only be used for easy money transfer between to persons, but also for exchanging other forms of data. In its newest version Ice Cream Sandwich the Android OS offers such feature called Android Beam (see Figure 5). Android developers can implement this option in order to transfer pictures, videos, websites or other data by simply holding two appropriate phones together. [23]

3) Product Information System: In [27] engineers at the ETH Zrich propose an NFC-based product information system for retailers named Mobile Sales Assistant. Products, e.g. articles of clothing, are equipped with a NFC tag allowing shop assistants to check availability and other related product data easily and to present the information immediately to the customer. It is imaginable to extend this prototype so that clients themselves can access product information and ratings with their own devices.

4) Location-based Wikipedia: Another approach of using NFC for information retrieval is given in [28]. It proposes a location-based mobile wiki by using NFC tag infrastructure. In a city, users can thus read local information content of places of interest from a Wikipedia system by touching certain tagged hotspots placed around the city with their NFC enabled mobile phone. It is suggested that this wiki data can not only be seen, but also be edited and updated by the users.

5) Indoor Navigation System: NFC tags can also be used directly for positioning services. In particular, the realization of indoor navigation systems is still quite sophisticated as GPS signals for instance are not accurate enough for those purposes or even not receivable at all. In [29] a system is presented that uses NFC tags spread over a building to provide seamless positioning and navigation indoors. When touching such tag with his device a map with a marker at the current position is downloaded and displayed. The user can select a destination and the optimal route is shown on the map.

6) Educational Systems: Other prototypes illustrate the usage of NFC in the field of education for example by building a contactless university examination system [30]. Courses and exam dates can be published on tagged smart posters. Students register for a course or an exam by waving their NFC phone over the adequate poster. Each NFC phone's Secure Element contains a virtual student card. The required data can thus be transferred to a central university server. Before starting the exam, the teacher identifies and verifies the attendant students by reading their NFC phones. As proposed in [31], this system can even be expanded to a huge intelligent "University of Things" allowing all kinds of booking facilities, access to library and computer rooms, books borrowing, photocopying, course information retrieval et cetera by making use of the NFC technology. A pilot project offering a set of such options is apparently already running at the University of Cordoba.

7) Medical Applications: Last but not least, several research projects investigate the advantages provided by NFC in the field of medical applications. A promising approach proposes various methods of health monitoring and recording of health status of patients by using NFC [32]. In hospitals at present usually a paper-based patients file needs to be carried around all the time providing the medical personnel with the patients status and medication. By outfitting patients with wearable NFC sensors, e.g. in form of a bracelet, a system could be established that allows medical assistants to collect data from patients by simply touching their bracelets. Furthermore, the data could be automatically transferred to a database that stores the patients records permanently. Another survey suggests to use NFC with mobile phones and RFID bracelets in developing countries to track large number of patients and material at low cost, especially in terms of disease surveillance [33].

Numerous companies and developers have clearly recognized the huge potential of NFC applications and try to invest big efforts into pushing this technology forward. One can assume that the most significant and most likely trend leads towards transforming NFC enabled mobile phones into virtual wallets. This progress is driven by many major and influential industries and is most applicable for the mass market and the average consumer. It will presumably result in the partial elimination of plastic payment cards, ID cards, coupons and other forms of tickets. At some time, even further typical wallet items like driver-license, passports or national identity cards could be integrated into NFC smartphones. Other appliances like using NFC for location-based services or monitoring processes are useful but will remain a niche market.

It is obvious that a successful propagation of such NFC applications relies on overcoming certain challenges, conflicts and problems. These will be addressed in the following final chapters.

IV. Security Concerns

As mentioned, most NFC scenarios are required to deal with sensitive data like credit card numbers, bank account details, account balances, personalized tickets or other personal data. For data storage and wireless data transfer security is therefore an essential issue. NFC thereby provides several mechanisms for security and immunity. First of all, there is obviously a certain physical security due to the touch-to-connect principle. As a matter of fact, the NFC technology only provides data transfer between two devices or between a device and a tagged object when the distance between the two items falls below a certain range. The usual transmit power of radio frequency and the receive sensitivity of NFC readers that fulfill the previously described ISO specifications are only strong enough to operate up to a range of a few centimeters. That means that e.g. at a supermarket checkout the customer needs to place his phone directly over the reading device. Data skimming, that is capturing and intercepting transferred data by a distant attacker, is hence not possible that easily. Misuse is however possible in the form of relay attacks [34]. Such attack is basically accomplished via an attacker serving as a man-in-the-middle who is forwarding transmitted data between a reader, e.g. a reading device for NFC payments, and a target transponder, e.g. a NFC device serving as a credit card, that is actually out of the reading range. The following example illustrates the procedure: An attacker places his modified NFC phone on top of the NFC reader at the POS, e.g. at a checkout in the supermarket. The phone however forwards the data, e.g. via Bluetooth, to his distant accomplice holding another modified NFC phone. He in turn holds his phone - without attracting attention - next to a contactless NFC smart card, e.g. NFC credit card, of the attacked target person. The accomplice's phone operates as NFC reader simulating the actual reading device at the POS. The reader at the POS assumes the target person's card is close, and unknowingly debits his account. The additional data exchange and forwarding via the attacking person-in-the-middle however naturally takes some extra time. A possible countermeasure for such relay attack could for example be built upon a quite short timeout threshold that avoids transactions if the response time is too slow. The concept of Google Wallet is however also secured against such attacks as thereby a PIN has to be entered in order to activate the phone's NFC broadcast hardware and to activate the Secure Element that is storing all the sensitive data. The Wallet PIN also prevents unauthorized usage of the payment card in case the NFC phone is stolen.

For the wireless channel communication itself the NFC specifications do not ensure any secure encrypting mechanisms. On higher layers however, NFC applications can of course use industry-standard cryptographic protocols like SSL/TLS based methods to encrypt the data that is to be transferred over the air and that is stored in the Secure Element. Other possible NFC vulnerabilities involve the manipulation of NFC tags [35]. Existing passive NFC tags, e.g. on a smart poster, could be replaced by spoofed tags such that a modified NDEF message is read by a NFC reading device. Possible attacks could for example replace the URI record with a malicious URL, e.g. in order to make the user load a phishing website that steals the users credentials. Experiments show that one can modify the NDEF message of a smart poster such that the visualized content on the phone, e.g. the website URL, is hardly distinguishable from the original one. Furthermore, it is even possible to create a malformed NDEF message that causes the some applications to crash. This form of manipulation could be used by attackers to debase the relationship between a user and the pretended service provider. The Signature Record Type that was previously addressed in this paper and that signs a whole NDEF message can however serve as a countermeasure against URL spoofing and similar attacks. By manipulating the signed tag payload a signed NDEF message will lose its integrity and will be recognized as not-trusted.

In general, one can summarize that NFC is not more insecure than other related technologies. It offers options for encrypting data on the application layer the same way as Wi-Fi or Bluetooth, but additionally provides safety through the requirement of very close physical proximity. Compared to traditional payment methods including magnetic strip cards that can easily be skimmed or cloned, it is quite difficult to tamper NFC hardware. Beside the physiological concern of transferring money or sensitive data without wired connection over the air, the NFC technology can thoroughly be considered as secure enough for mobile ticketing and payment - at least, if the application developers make use of the provided security mechanisms. And in order to manage existent psychological discomfort, customers just need to be educated in more detail about the technology and its reliability before using it.

V. Challenges and Discussion

At present, the NFC technology has reached a level where commercial launch preparation can begin and should be established. However, to some extent definite standards for NFC services are still missing. The lack of an ultimate conclusive strategy for the development of NFC services originates in a vital conflict between several involved key actors including mobile phone manufactures, network operators, banks and other service providers: every party indeed tries to enforce its interests and wants to play a major role in the flow of the application scenario and the associating acquisition of big money. Third-party providers, like banks and other financial institutions, want to host NFC applications in neutral space on the handset, whereas network operators of course want to charge customers for providing services hosted in secure environment on the UICC. They are also in possession of the underlying wireless network infrastructure and can thus control any SMS-based remote over-the-air management capabilities that might be used to conveniently configure or update NFC services on the handset. The mobile phone manufacturers on the other hand decide which sort of NFC hardware and which alternative forms of dedicated Secure Element chips are actually implemented in the handset. And on higher layers, of course also the phone's operating system needs to provide appropriate NFC support. Google already offers mature NFC interfaces for developers within their own Android operating system and - in partnership with several banks and the assistance of a handset manufacturer - managed to publish a fist qualified application for mobile NFC payment. Competitors from Apple and Microsoft indeed also announced plans to develop smartphones with NFC support in the near future, but it is still unsure how exactly their concept will look like. Nevertheless, this means that NFC applications are still handset specific. A simple, dynamic and platform-independent framework is missing and difficult to realize. In a certain way though, a collaboration of stakeholder, in particular phone manufacturers and network operators, is definitely needed for developing sophisticated and usable NFC services for the mass market. [14], [36], [37]

Reliability and usability of NFC applications are probably the most important determinants of the user experience in everyday use of the NFC technology and therefore important keys to its success. When compared to alternative technologies, NFC offers great advantages. Essential corner stones have already been established and effectual field trials have been completed. Now, based on successful partnerships and collaborations between the mentioned stakeholders, applications with good user experience need to be published. The existence of such applications is attended by the motivation of handset manufacturers to be incentivized to the production of NFC capable smartphones. Having this accomplished, it is very likely that the NFC technology will play a big role in our future everyday life.

References

[1] G. International Telecommunication Union (ITU), "Itu internet reports 2005: The internet of things, executive summary," november 2005, last visited on January 19th 2012. [Online]. Available: http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf

[2] I. C. USA, "Idc - press release: Samsung takes top spot as smartphone market grows 42.6visited on January 19th 2012. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUS23123911

[3] ——, "Idc - press release:smartphones outstrip feature phones for first time in western europe as android sees strong growth in 2q11, says idc," september 2011, last visited on January 19th 2012. [Online]. Available: http://www.idc.com/getdoc.jsp?containerId=prUK23024911

[4] J. Langer and M. Roland, *Anwendungen und Technik von Near Field Communication(NFC)*. Springer, 2010.

[5] R. Want, "Near field communication," *Pervasive Computing, IEEE*, vol. 10, no. 3, pp. 4 –7, march 2011.

[6] K. Ok, V. Coskun, M. Aydin, and B. Ozdenizci, "Current benefits and future directions of nfc services," in *Education and Management Technology (ICEMT), 2010 International Conference on*, nov. 2010, pp. 334 –338.

[7] Image source. [Online]. Available: http://www.sagedata.com/images/2007/RFID%20Tag%20HF.jpg

[8] M. Roland and J. Langer, "Digital signature records for the nfc data exchange format," in *Near Field Communication (NFC), 2010 Second International Workshop on*, april 2010, pp. 71 –76.

[9] M. Reveilhac and M. Pasquet, "Promising secure element alternatives for nfc technology," in *Near Field Communication, 2009. NFC '09. First International Workshop on*, feb. 2009, pp. 75 –80.

[10] F. Reynolds, "Whither bluetooth?" *Pervasive Computing, IEEE*, vol. 7, no. 3, pp. 6 –8, july-sept. 2008.

[11] B. Schilit and U. Sengupta, "Device ensembles [ubiquitous computing]," *Computer*, vol. 37, no. 12, pp. 56 – 64, dec. 2004.

[12] C. Gaylord, "Google wallet: Shop with a swipe of your phone," september 2011, last visited on January 19th 2012. [Online]. Available: http://www.csmonitor.com/Innovation/Tech/2011/0920/Google-Wallet-Shop-with-a-swipe-of-your-phone

[13] G. P. Ltd, "Google wallet - faq," 2011, last visited on January 19th 2012. [Online]. Available: http://www.google.com/wallet/faq.html

[14] J. Zou, C. Zhang, C. Dong, C. Fan, and Z. Wen, "Mobile payment based on rfid-sim card," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 29 2010-july 1 2010, pp. 2052 –2054.

[15] MasterCard, "Mastercard paypass," 2012, last visited on January 19th 2012. [Online]. Available: http://www.mastercard.com/de/privatkunden/products/products_paypass.html

[16] L. Leavitt, "Polyamorous google wallet adds visa to its arsenal," september 2011, last visited on January 19th 2012. [Online]. Available: http://www.engadget.com/2011/09/20/polyamorous-google-wallet-adds-visa-to-its-arsenal/

[17] A. F. de Azevedo Figueiredo Cruz, "Nfc and mobile payments today," november 2011, last visited on January 19th 2012. [Online]. Available: http://www.di.fc.ul.pt/∼nuno/THESIS/AndreCruz_MSIT11.pdf

[18] W. W. Maisie Ramsay, "Isis explains strategy shift," may 2011, last visited on January 19th 2012. [Online]. Available: http://www.wirelessweek.com/news/2011/05/Isis-Explains-Strategy-Shift/

[19] V. Savov, "Isis nfc payment system gets its first market in salt lake city, utah, launches in 2012," april 2011, last visited on January 19th 2012. [Online]. Available: http://www.engadget.com/2011/04/06/isis-nfc-payment-system-gets-its-first-market-in-salt-lake-city/

[20] X. Yu-ning, "Research on nfc and simpass based application," in *Management and Service Science, 2009. MASS '09. International Conference on*, sept. 2009, pp. 1 –4.

[21] Watchdata, "New wave in mobile payment, watchdata simpass has done it again," march 2011, last visited on January 19th 2012. [Online]. Available: http://www.watchdata.com/press/10212.html

[22] n. Sarah Clark, "Paypal launches nfc p2p payments service," november 2011, last visited on January 19th 2012. [Online]. Available: http://www.nfcworld.com/2011/11/08/311197/paypal-launches-nfc-p2p-payments-service/

[23] J. Stern, "Android beam: pictures, video and hands-on," october 2011, last visited on January 19th 2012. [Online]. Available: http://www.theverge.com/2011/10/19/android-beam-pictures-video-hands-on/

[24] N. F. Inc, "Nfc in public transport," january 2011, last visited on January 19th 2012. [Online]. Available: "http://www.nfc-forum.org/resources/white_papers/NFC_in_Public_Transport.pdf"

[25] B. Dobson, "Nfc in transport for london," july 2008, last visited on January 19th 2012. [Online]. Available: http://www.nfc-forum.org/resources/presentations/Brian_Dobson_Transport_for_London.pdf

[26] T. R. Bill Ray, "Credit cards at the turnstile across london by 2013," february 2011, last visited on January 19th 2012. [Online]. Available: http://www.theregister.co.uk/2011/02/25/tfl_nfc/

[27] S. Karpischek, F. Michahelles, F. Resatsch, and E. Fleisch, "Mobile sales assistant - an nfc-based product information system for retailers," in *Near Field Communication, 2009. NFC '09. First International Workshop on*, feb. 2009, pp. 20 –23.

[28] E. Siira, T. Tuikka, and V. Tormanen, "Location-based mobile wiki using nfc tag infrastructure," in *Near Field Communication, 2009. NFC '09. First International Workshop on*, feb. 2009, pp. 56 –60.

[29] B. Ozdenizci, K. Ok, V. Coskun, and M. Aydin, "Development of an indoor navigation system using nfc technology," in *Information and Computing (ICIC), 2011 Fourth International Conference on*, april 2011, pp. 11 –14.

[30] B. Sodor, G. Fordos, T. Doktor, and B. Benyo, "Building a contactless university examination system using nfc," in *Intelligent Engineering Systems (INES), 2011 15th IEEE International Conference on*, june 2011, pp. 57 –61.

[31] G. Miraz, I. Ruiz, and M. Gomez-Nieto, "How nfc can be used for the compliance of european higher education area guidelines in european universities," in *Near Field Communication, 2009. NFC '09. First International Workshop on*, feb. 2009, pp. 3 –8.

[32] H. Zhang and J. Li, "Nfc in medical applications with wireless sensors," in *Electrical and Control Engineering (ICECE), 2011 International Conference on*, sept. 2011, pp. 718 –721.

[33] A. Marcus, G. Davidzon, D. Law, N. Verma, R. Fletcher, A. Khan, and L. Sarmenta, "Using nfc-enabled mobile phones for public health in developing countries," in *Near Field Communication, 2009. NFC '09. First International Workshop on*, feb. 2009, pp. 30 –35.

[34] L. Francis, G. P. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones." *IACR Cryptology ePrint Archive*, vol. 2011, p. 618, 2011. [Online]. Available: http://dblp.uni-trier.de/db/journals/iacr/iacr2011.html#FrancisHMM11

[35] C. Mulliner, "Vulnerability analysis and attacks on nfc-enabled mobile phones," in *Availability, Reliability and Security, 2009. ARES '09. International Conference on*, march 2009, pp. 695 –700.

[36] B. Benyo, "Business process analysis of nfc-based services," in *Computational Cybernetics, 2009. ICCC 2009. IEEE International Conference on*, jan. 2009, pp. 75 –79.

[37] A. Dubey, M. Giri, M. Sahare, and A. Dubey, "Step-up analysis and generalization approach for trusted nfc application development for enhancing real time use location," in *Communication Systems and Network Technologies (CSNT), 2011 International Conference on*, june 2011, pp. 318 –322.