International Journal of Electrical and Computer Engineering (IJECE)
Vol.2, No.3, June 2012, pp. 371~382
ISSN: 2088-8708

Near Field Communication

Kevin Curran, Amanda Millar, Conor Mc Garvey
School of Computing and Intelligent Systems
University of Ulster, Magee Campus, Northern Ireland, BT48 7JL, UK

Article Info

Article History:

Received Jan 20th, 2012
Revised Apr 10th, 2012
Accepted Apr 24th, 2012

Keyword:

Commercial services
Communication
NFC
Smartphone
Wireless network

ABSTRACT

Near Field Communication (NFC) is a technology that enables a device to communicate with another at a maximum distance of around 20cm or less. Currently, mobile phone manufacturers, banking institutions and mobile network providers are attempting to apply this technology to Smartphones and other handheld devices because of the opportunity to enable the consumer to use commercial services more easily. This paper discusses the expected increase in mobile payments using Near Field Communication, possible uses and the risks associated with carrying out transactions over a wireless network. We also discuss a real world implementation of an NFC based loyalty card system for retail.

Corresponding Author:

Kevin Curran,
S School of Computing and Intelligent Systems,
University of Ulster, Magee Campus, Northern Ireland, BT48 7JL, UK,
Email: kj.curran@ulster.ac.uk

1. INTRODUCTION

Near Field Communication (NFC) is a specification for contactless communication between two devices. NFC is based on the technology used for RFID and is standardised in ISO/IEC 18092. It is limited to a distance between the two devices of up to 10 cm. NFC is intended to make it easier and more convenient to make transactions, exchange digital content, and connect electronic devices with a touch [1]. NFC operates at 13.56 MHz and has been developed jointly between NXP Semiconductors (formerly Philips Semiconductors) and Sony Corporation [2]. Because NFC has the ability to read and write to devices, it is believed that they will have a wider use in the future than standard smart cards. NFC involves an initiator and a target. The initiator, as follows from the name, initiates and actively generates an RF signal and controls the exchange of data (a payment device) where the request is answered by a passive target (a Smartphone). The NFC protocol also distinguishes between two modes of communication: active and passive. Active is where both the initiator and target both communicate by generating their own electric fields. They do this in half duplex; deactivating their RF field until no other device is transmitting. In this mode both devices will typically have power supplies. Passive mode will be the more common application in where the initiator is the only device that generates an RF signal, the target device answers that call by modulating the existing field which the initiator device listens out for, and then processes therefore transferring data. The data rates currently supported are 106, 212, 424 or 848 Kbit/s

Barclaycard introduced the UK's first contactless payment system in 2007, with a transaction limit of £10. Due to the increase in demand, Barclaycard increased the maximum limit by 50% to £15 in 2010. Google has supported the incorporation of NFC into the Android 2.3 operating system and it is predicted that over the next three years the market for NFC chips will grow by a factor of four, and in 2011, 50 million NFC-enabled devices will enter the market [3]. With the increase in ownership of smartphones over recent years, people are relying more heavily on their phones to be able to support their everyday activities. Since the launch of the revolutionary iPhone in June 2007, the public's need for apps has increased and it is now possible to get an app for practically anything. The smartphones are multi-functional devices that act as more

than a phone: most have cameras or video functionality, music players, web-browsing capabilities and GPS navigation. With the increase in popularity of social networking sites such as Facebook and Twitter, most users now require the additional functionality of being able to communicate with their friends in real-time using web-enabled phones.

As users' needs for technology increase, it makes sense that another function to add would be the ability to use the device to make payments, and that is where NFC comes in. Having a mobile phone fitted with an NFC chip will enable users to send and exchange data just by touching, or bringing together the two devices. Figure 1 shows the NFC-related elements on Mobile Handsets.

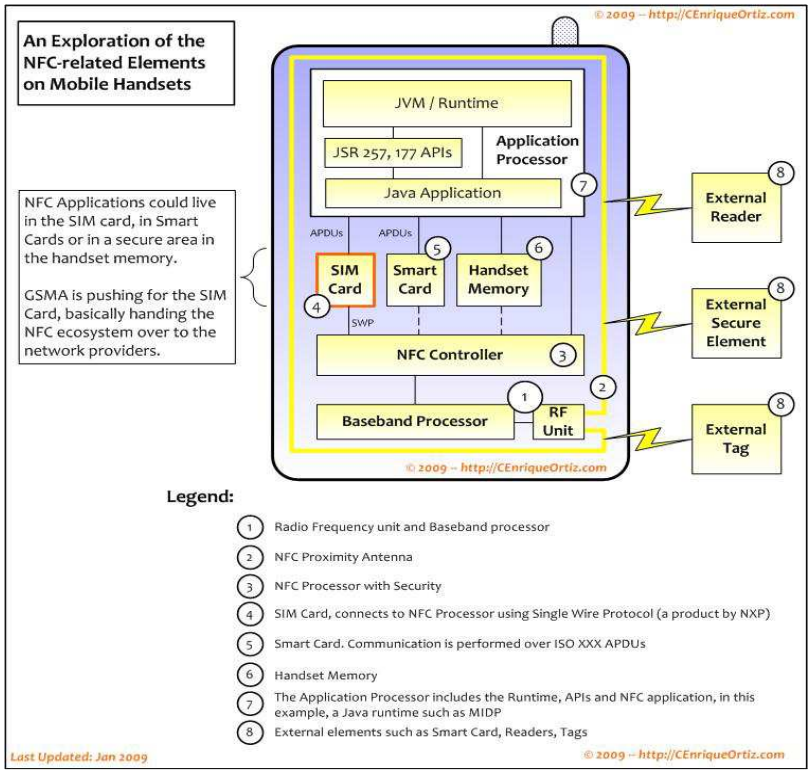

Figure 1. Exploration of the NFC-related elements in mobile handsets [4]

There is a choice of where the NFC applications can be stored on the phone: on the SIM card, within the smart card or even within an area of the phone's memory. If the NFC applications are stored within the SIM cards, then this passes control over to the network providers, rather than the handset manufacturers. Having the applications on the SIM card would make the SIM the secure element for the authentication protocol and provide portability between handsets.

The mobile phone has become one of the most successful inventions of the 20th Century [5] becoming one of the major communications device in the late 1990s. The development for mobile phones started as far back in the 1940s, shortly after the end of World War II. Bell Laboratories combined two technologies the telephone and the radio. They also were behind the concept of cellular communications, with their ideas about reusing radio frequencies between hexagonal cells [6]. It is because of the development of the cellular networks that mobile communication has been able to be such a success, although initially the cost of making a call was prohibitive to the majority of people. The first mobile phone call took place in New York on 3rd April 1973 when Martin Cooper, General Manager of Motorola called his rival at AT&T Bell Labs, Dr Joel S Engel. It took a further ten years of investment in research and development before the first commercial mobile phone, the Motorola DynaTAC 8000x, was released at a cost of nearly $4,000 each.

2. NFC STANDARDS

NFC is an international accredited standard, which means that in the future it will become a worldwide-recognized technology with a multitude of uses. In December 2003, NFC was accredited with the standard ISO/IEC 18092 (NFC IP-1). This standard specifies the interface and protocol for simple wireless communications between close-coupled devices that communication with transfer rates of 106, 212 and 424 kbps [7]. In 2005, NFC also earned a further internationally accredited standard ISO/IEC 21481.Figure 2 shows the ISO standards that the NFC standards support.

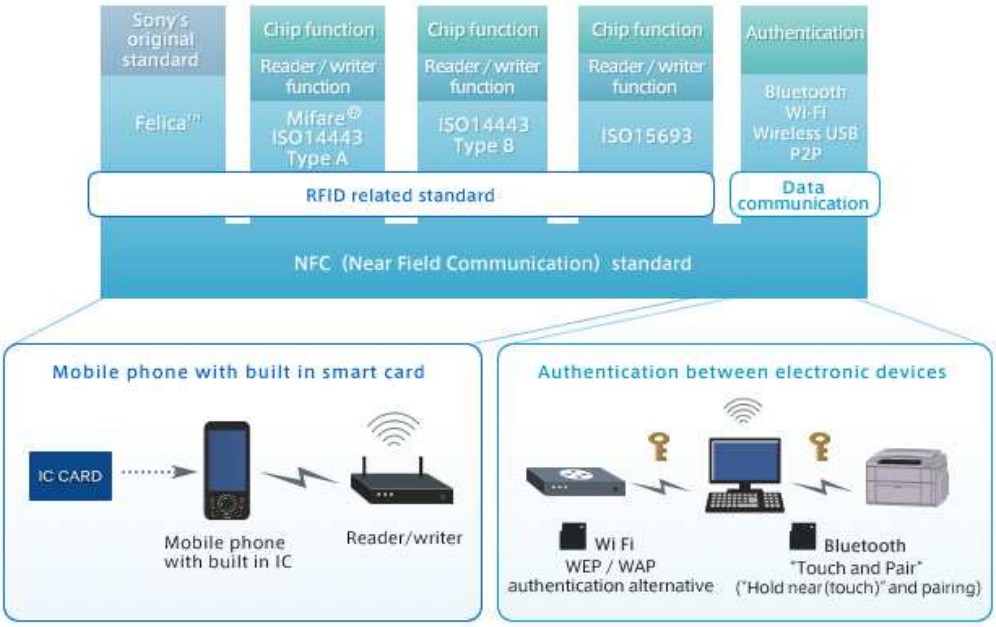

Figure 2. Near field communication standards [2]

Secure NFC combines smart-card technology with NFC technology to enable storage of personal data in a secure manner. This means that data can be encrypted, with the key being stored securely in the memory of the device and the NFC device supports the authentication. This secure storage will be required to store personal data, encryption keys, electronic money etc., and so it is an important aspect of the NFC-enabled device. Enhanced NFC is a feature that makes a transaction possible, even if the mobile is switched off or the battery is drained, which would be important for instances such as ticketing.

For a device to work using NFC, a chip is installed into a mobile phone. If the application involves payments, the chip is linked to a credit or debit card account so that money can be charged to the user's account. To make a payment using the NFC enabled mobile, the user swipes the mobile over a contactless pay point, from a distance not exceeding 10 cm. This action will then charge the debit or credit card that has been linked to the chip inside the phone. Currently, there is a maximum limit of £15 per transaction on NFC transactions. Using NFC also enables the user to configure Bluetooth connections for faster transfer. The devices work in two modes: passive and active. This works on the concept of a message and reply. The active or initiator device sends a message to the passive, or target device. The target device then responds, but can only do so once it has received the message from the initiator. The code that is transmitted between the two devices uses Manchester coding. It is possible for the active device to take on both active and passive roles, but the passive device is always the target. The initiator will send a message to the target and then wait for a response.

3. NFC APPLICATIONS

As more phone manufacturers start to include NFC chips in their mobiles, the need for applications will increase. Already marketers are looking at the possibilities of using the NFC interface alongside their traditional marketing methods such as posters. Information could also be passed to the NFC device, allowing the user to gain more information about a product or service, so this would be an efficient means of advertising. For example, it would be possible to transmit a URL to the target device so that the user would then be able to navigate to a website to get further information about a product or service in which they are

interested. This is where having NFC enabled on a smartphone could prove to be very useful for consumers, enabling them to find out the best price for a product before committing to the purchase. There are many uses for NFC apart from the small Point of Sale (POS) transactions mentioned previously. They can also be used to transfer tokens at airports, which would eliminate the need for boarding cards. The passenger would check-in using their mobile and then re-confirm by swiping their phone again at the departure gate. There is also the possibility of them being able to store biometric information, which is becoming more widely developed for security at airports.

NFC devices can be used in conjunction with image display devices like digital photo frames for displaying images very quickly. All the user needs to do is touch the photo frame with the image ready to be sent, then the connection is established and the image is sent over Bluetooth. NFC is backward compatible with RFID therefore it is perfectly feasible to use an NFC enabled device as an RFID key. This can be used with traditional RFID access control systems as a replacement for the key fobs and cards currently used. Wireless car keys using NFC are being developed by BMW with personalized settings stored into each key. They have developed an NFC car key system which will link into the cars current navigation system which already allows for hotel reservation, and train ticket booking. Using NFC the tickets and reservations can now be stored on the NFC card which can then in turn be used to gain access to the hotel room or validate the ticket with the conductor. Applications for smartphones are starting to appear that allow the user to create their own NFC tags, an application that was developed and is being distributed for free is NXP Tag Writer for the Android smartphone. The application uses the NFC enabled phone to send a signal to write contact details, URLs and SMS messages onto an NFC enabled tag which can be on items like business cards up to posters.

Figure 3: Day in the life of NFC [8]

Figure 3 above details just a few of the ways that NFC can be used in our everyday lives. This demonstrates the potential uses for NFC-enabled devices. Mobile phone manufacturers are currently carrying out Field tests into a variety of NFC applications. In February 2011, Transport for London (TfL) confirmed plans that it would be accepting contactless payment cards over its whole network, in time for the 2012 Olympic Games [9]. By adapting their current Oyster Card system, TfL will make the transport system more accessible to both domestic and international visitors. Android 2.3 was released on 6th December 2010 and

one of the changes included support for Near Field Communications. This enabled Android developers to create a whole new class of applications that will make use of the newly supported technology. With widespread support now available NFC will soon be established as a practical technology for smartphones and other widgets, like Bluetooth is today with modern handsets.

The future of NFC seems to be fruitful as it is currently getting support from the major smartphone stakeholders (Apple's iPhone, Google's Android and Microsoft's Windows Phone 7) as they compete for a share of the mobile operating system market. ABI research estimate that devices with NFC will double in 2012, from 35 million shipped in 2011.

Devices with applications that use NFC technology for payments will help consumers pay for products and services more easily, and mobile developers are teaming up with financial companies and service providers to provide this service in the near future. Global payments company Visa is collaborating with mobile manufacturer Samsung to bring NFC 60,000 merchants in London for the 2012 Olympic Games. NFC is also being developed for contactless ticketing. With an NFC enabled phone the consumer can purchase a bus/event ticket, download it and when at the gate, use the device to gain access to the event/bus or train. This is currently being trialed in several European cities including Transport for London's underground that are rejecting the current NFC as too slow for people rushing to get to the tube. NFC will bring interactive advertising a level never achieved before as it will enable the consumer to 'pull' information from an advertisement, eliminating the passive role traditionally held by the consumer. A smart poster is a poster embedded with an NFC tag which will provide the consumer with more information on the product. The capacity of an entry level tag is very limited with 1kb and 32kb for the most expensive option. Therefore it will only really be able to hold a web address of the advertised product. In this case the device may open a browser window and connect to the internet to retrieve the web page or display text in the format of a text message, image and especially video which may not be cost effective to have at this time. Retailers will have an advantage as they will have the opportunity to detect how many customers respond to what ad and in what magazine. It will be a good tool which advertisers can use to measure how effective their advertisement was. Consumers will be able to redeem virtual coupons, collect loyalty points and download discounts from websites instead of bringing a hard copy to the high street store. The buyer can then redeem the appropriate coupon by using their smartphone and the stores NFC reader. It seems that NFC is set to stay, according to research firm Gartner as they estimate that in 2014, 340 million global wireless clients will use mobile payments.

4. NFC SECURITY ISSUES

It is estimated that the market in NFC devices will grow exponentially [10] over the next few years, and with this comes the always-present issue of security. The requirement for the two devices to be close to each other is something that helps with the security of the transaction by limiting eavesdropping. The range of NFC is only a few centimeters. This makes it inherently safer than longer range technologies but there are still security flaws that, if not addressed, can be exploited. According to the ISO standard, NFC is not encrypted. This is to make it backward compatible with RFID technologies. Encryption may be implemented with future NFC applications but only as a best practice, not as a requirement. The wireless signal generated by data transfers can be picked up by antennas, modified, and dispatched. This makes NFC inherently vulnerable to this kind of attack. In active mode where the two devices are communicating, eavesdropping is significantly easier compared to passive mode as the antenna signal gain is lower, therefore the listening range is greatly decreased. It has been found that when in it is easy to successfully eavesdrop from around 30cm. The AES encryption method is developed into a series of NFC security standards to protect against eavesdropping and data manipulation. An NFC skimmer device, similar to the magnetic strip skimmer used in ATM machines could be possible to implement. With a disguised device placed close to the two NFC devices, it would be able to record all NFC activity in a given time and be collected at a later date. NFC is starting to become popular as a form of advertising, where the interested user taps their device onto the advert to view the message, URL or phone number. Fraudsters can take advantage of NFC tags in public places by removing the legitimate tag and replacing it with a tag directing the user to a bogus website of a premium number set up to the fraudsters' account. Using a wireless communication protocol it is inevitable that the data will be prone to attack such as:

4.1. Eavesdropping

The two NFC devices communicate using radio-frequency waves. This means that an attacker could use an antenna to intercept the transmitted signals. No special equipment is required to receive or decode the RF signals, and so it should be assumed that this equipment is available to attackers. It is harder to eavesdrop on a passive target device, because they do not generate any RF fields. It is possible to

eavesdrop on the active device from a distance of up to 10m when it is in transmission mode, but this reduces to only 1m when the device becomes passive.

4.2. Data Corruption

Rather than eavesdropping on the communication, an attacker might instead try to modify the data being transmitted. The attacker may do this to disrupt the communication by preventing the receiving device from being able to understand the data that is being transmitted from the active device. This method of attack works in the same way as a Denial of Service attack, by preventing the communication being completed between the two devices.

4.3. Data Modification

This type of attack is more difficult to carry out because it is dependent on the strength of the amplitude modulation. The purpose of data modification is to change the data that is received rather than preventing the transmission as with the data corruption attack, because the attacker wants to make changes to the data that is being transmitted.

4.4. Data Insertion

This is only possible if the answering device is slow to respond to the message sent by the active device. The attacker inserts messages into the data exchanged between the two devices, but if the messages overlap, then the data becomes corrupt and the communication fails.

4.5. Man-in-the-Middle Attack

In this type of attack is the two devices are tricked into believing they are communicating directly with each other, when in fact they are communicating through a third party. The two devices are not aware of the third party and so any data exchanged will be accessible to the device in the middle, and hence the name “Man-in-the-middle”. However, because of the way that NFC devices use a message and reply protocol, it is deemed virtually impossible to set up a man-in-the-middle attack. This is because it is impossible to align perfectly two RF fields and the attack would be discovered.

Another aspect to protect against is ‘Walk off’. Walk offs are when the device user lifts the device and walks away from the transaction while leaving the transaction connection open. Usually, when the connections are idle for an amount of time the connection terminates automatically, but the time window where the connection is still open, it can be exploited. A wireless key can be used to encrypt the data. Also a new concept is ‘Electronic Leash’ which terminates the connection once the device senses a set distance has been exceeded. Devices using NFC are expected to operate in environments with varying security, some with a high level of security and others that do not need any security. As the NFC Forum has repeatedly stated the technology is ‘inherently secure’ because of the small transmission distance. The best solution to these security issues is to have a layered security model with a minimum requirement of authentication before the start of communication. Developers can then add higher levels of security according to their application needs. This is not required by the ISO standard but will be essential for making money from the technology.

5. NFC LOYALTY CARD CASE STUDY

RFID-enabled loyalty cards can provide loyal customers with services far beyond a typical loyalty card's price reductions. A well implemented system can link to a network-based system to dole out such benefits as recall notifications, refunds of prices that drop following a purchase, and refund credit for items shoppers were dissatisfied with. An RFID loyalty card system can also enable customers to manage their shopping experience on the store's Web site, where patrons can input a shopping list, track previous purchases and sign up for discounts later provided at the point of sale. Some excellent schemes offer elements such as a low-price guarantee that automatically provides customers with a credit whenever an item's price is reduced within seven days after that purchase is made therefore the credit is then applied to the shopper's next purchase cost. An RFID smartcard system could also allow for automatic refunds in the case of purchasing a spoiled item. If, for instance, a customer takes a liter of milk home and discovers it has gone bad, they can call the shop, provide their card ID number and receive credit automatically. Other novel elements can also be introduced by IGONOGO clients such as automatic recall notification which might involve sending an alert to all customers who have purchased a product that has been recalled, and warning them that the specific item does not meet shop standards, or that is being recalled by the vendor and should be discarded. To enable this, shops can have RFID interrogators installed at cash registers that can capture

the ID number of a card positioned from a few centimeters away or doorways that capture a card from yards away.

There is an option of using technology such as bar-code or mag-stripe options for smart cards however RFID provides greater security than mag-stripe technology because personal data is never exposed, and remains in the back-end system, with only the encrypted ID number transmitted. This means that more options are available to customers, such as paying for purchases by presenting only the loyalty card, as well as connecting other customer data to that card, based on information input by the patron on his or her personalized Web page. Retailers can then use it to provide coupons to loyal customers, or to entice those who would not be considered loyal shoppers. In the future, customers could input information such as a shopping list. If the shop then installs a monitor and RFID interrogator near its entrances, a customer could utilize that service to access their shopping list upon arrival, and receive details such as where needed items are located, along with which brands are on sale. The system can also enable customers to instruct it to automatically deduct a transaction cost from a credit card or debit card, thereby enabling them to pay for transactions with the loyalty card alone.

World Cup tickets have had embedded RFID tags since 2006. The relative small increase in cost of using RFID over conventional football tickets is outweighed by the additional security provided. These new tickets not only make it almost impossible to copy but at any given time the FIFA will know the name, address, birth date, nationality and ID card/passport number of all fans watching the World Cup in all the stadiums at any one time. Coffee Republic (UK), were one of the first to introduce a combined contactless payment and loyalty-card system (NFC from sQuid) Not only did the introduction of these cards shorten waiting times at the sales counter and increase consumer loyalty, it also provided the company access to its customers by demographic or in general anonymously e.g. to determine the ages or genders of customers at any particular location or time within any of their stores. An agreed cost of the sQuid card usage works out to be around 1.5% of the total cost of a typical purchase meaning it costs no more than a typical merchant trader credit/debit card fee.

One of the first contributors to public skepticism to RFID cards in relation to privacy issues can be traced back to 2004 in Germany. A retail group in Germany did made a blunder when they introduced RFID into their loyalty cards without telling customers. Metro (Germany) issued a UHF RFID loyalty card whereby customer shopping habits were recorded every time they visited a store. The privacy issue has since developed into an ongoing battle between developers and hackers – particularly with NFC bank cards using for example Visa's payWave technology. Latest scaremongering tactics from hackers show the use of a (freely available for under £100) portable NFC scanner connected to a laptop can ‘scan’ basic details of a bank card type, the branch and customer name from anyone standing close enough, for example in a bus, a queue, of walking too close. Avis (USA) recently introduced an RFID trial in America that aims to provide a new service of hourly, daily and one-way rental needs of corporate clients on-site. Not only does the introduction of RFID make the identification and tracking of vehicles more efficient, but it has more importantly, introduced a new market to develop and provided the opportunity to extend their hold on the current market share.

5.1. Loyal Customer Tracking in Retail Specification for Trial

This is a short outline of a loyalty card scheme for loyal customer tracking in the retail sector. The system uses an RFID hardware portal to track 'opted-in' customers in a shop. The RFID reader interfaces with a back-end customer loyalty database.

The initial trial took place in shop. There are numerous possible scenarios such as outlined in Figure 4. The important thing to note here is that they require a high accuracy rate for customers entering through the door. The read range is an indication of where tags might be read.

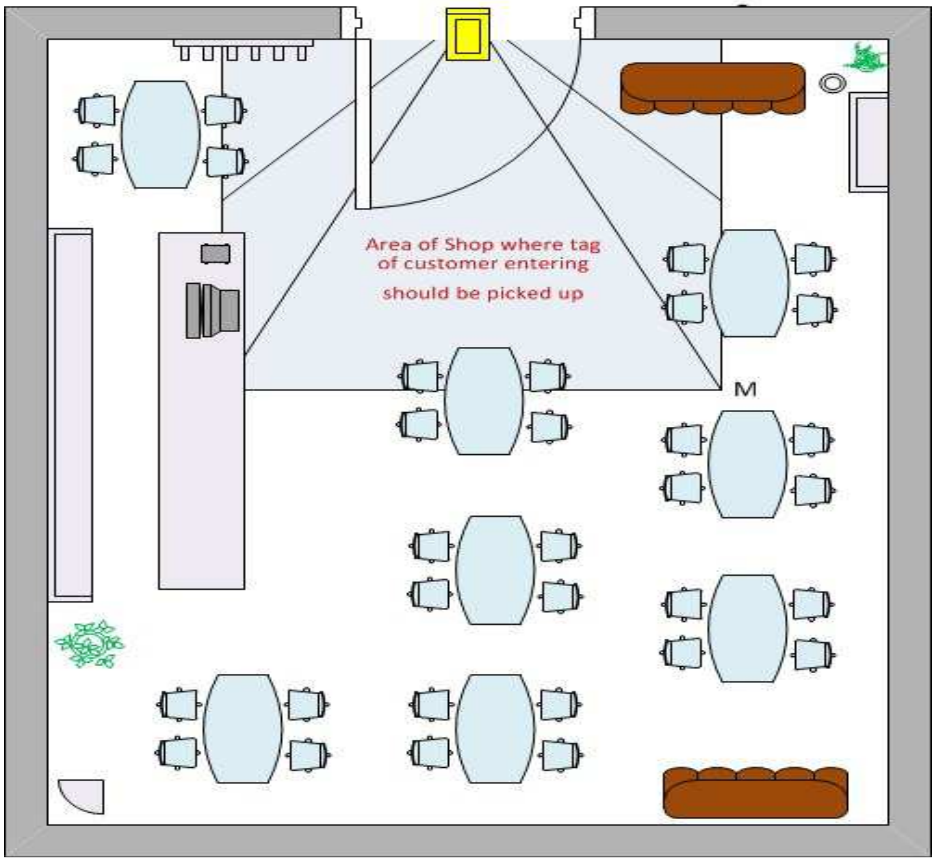

Figure 4. Layout of shop for initial feasibility study

Trial Preparation

Offsite

1. RFID tags applied to selection of medical records in warehouse.
2. Transfer van kitted out with Handheld RFID & Barcode readers

Shop

1. Entry/Exit fitted with RFID Reader Device Portal(s)
2. Power to/from RFID Portal(s)
3. RFID reader interfaced with loyal company database
4. Optional: Customer purchases linked to POS terminals

Equipment

1. RFID Entry/Exit Portal Reader(s)
2. RFID Tags, smartcards or keyrings
3. Cabling or wireless module to interface with backend system

Use Case Scenario - shop

Customer enters shop

1. New Customer enters shop
2. Customer tag read by portal reader
3. Customer added to database with timestamp

Customer leaves shop

1. Customer leaves shop
2. Customer tag read by portal reader
3. Time of customer leaving shop added to backend database

The company wished to implement the most cost effective and accurate system for tracking customers in a pilot study so as to commence a wider trial for commercial gain. The system should be capable of addressing the non-optional use case scenarios as described. The company has full access to the backend customer database. The company was ideally seeking a UHF solution with passive tags. HF solutions were also proposed and accepted due to the expected lower cost.

The recommended system was from Convergence Systems Limited (CSL) who is a Hong Kong based design engineering and sales company of RFID readers, antennas, RFID modules, and custom RFID tags. CSL's readers have built-in middleware and edge server application supporting EPC Gen 2 specifications. CSL also offers a full line of active RTLS RFID products. CSL was established to deliver a broad portfolio of RFID products to OEMs and system integrators around the world. CSL is a member of EPC global. The CS203 is a UHF EPC C1G2 Integrated RFID reader with long read range and high read rate (see Figure 5). In addition, the reader is offered with 8 different connectivity options: USB, RS232, RS485, Wiegand, Ethernet, WiFi, GSM/GPRS+GPS, and RTLS with +/- 1 meter resolution. These connectivity options make this integrated reader versatile and can be used in all environments, indoor or outdoor so is suitable for shop entrances.

Figure 5. CS203 RFID reader

The Convergence Systems Ltd (CSL) support also provided coding example - specifically Server Side Applications examples for the CS203 reader. These are a Unified C# API (Call-back based) Multi Application Demo, a CS203 Java API DemoApp and a Low Level API Software Package (C-based Linux Demo App).

Other relevant systems include CoreRFID who have a *Demo Kit UHF USB Pen Reader/Writer* designed for reading and writing all ISO 18000-6 Part B and C Tags. Its integrated configuration software enables it to operate with all the common UHF frequencies from 840 – 960 MHz (EPC Gen2), which makes it usable in Europe, US, and Asia. The UHF USB Read/Write Stick is an easy to handle RFID Reader to be used with USB equipped Terminals and Laptops. Its light weight and compact design, in combination with the latest technology and a robust ABS housing, make it the perfectly suited to a very wide range of identification applications.

The linearly polarized built-in antenna allows a maximum reading distance of up to 80cm. The USB V2.0 type A ensures reliable, high-speed data transfer. The reader supports data rates to the tag of between 40kbps and 250 kbps, and from the tag to the reader of 40kbps. The UHF Read/Write USB stick includes a multi-colour LED indicator to easily monitor the reading status. The reader uses the 5 Volt USB power supply, and the power output is adjustable up to 20dBm. Moreover, the Reader offers a reader sensitivity well over 90 dBm.

Figure 6. CoreRFID demo kit

This Demo Kit includes USB pen reader, demo software, software development kit, mixed samples of Confidex hard tags and mixed samples of Confidex labels and special tags. Example applications for this reader include logistics, tracking and tracing, product identification and distribution and inventory control.

6. POTENTIAL FUTURE OPPORTUNITIES

6.1 Google Wallet

Google Wallet is an Android app that makes your phone your wallet [11]. It stores virtual versions of your existing plastic cards on your phone. It works by people tapping their phone to pay and redeem offers using near field communication. It is just being rolled out around the world. Google Wallet has been designed for an open commerce ecosystem. It aims to eventually hold many cards people keep in their leather wallet today. Because Google Wallet is a mobile app, it will be able to do more than a regular wallet ever could, like storing thousands of payment cards and Google Offers but without the bulk. Google hope that eventually our loyalty cards, gift cards, receipts, boarding passes, tickets, even our keys will be seamlessly synced to our Google Wallet. And every offer and loyalty point will be redeemed automatically with a single tap via NFC. The vast majority of phones however do not support NFC but Google believe that NFC will be surging in popularity over the next couple of years, and for the time being this is really a first step. Google also has a plan to enable older devices to use a more limited version of the app - stickers that you can put on the back of your phone.

Figure 7. Google wallet

Google are a little vague to date on this but it seems the plan is that users will be able to obtain special NFC stickers with a single credit card associated with them (such stickers already exist, but these stickers will apparently be able to communicate with the Google Wallet app). Transactions made using the sticker will be relayed to the Wallet application on an Android device via the cloud. It is possible this functionality will be extended to other platforms as well, as Google says it is willing to partner with everyone to help broaden support for Google Wallet. Google Wallet is now released on the Nexus S 4G by Google. One can pay with Citi Master Card cards and the Google Prepaid Card. Customers can tap to pay at hundreds of thousands of merchants.

6.2 NFC and Windows 8

Microsoft's upcoming Windows 8 operating system (OS) will include built-in NFC functionality. Although Microsoft has yet to set a date for the product's release, the company reports that the new system will include an NFC function known as *"tap to share,"* enabling Windows 8 PCs, laptops or tablets to support NFC RFID readers. In that way, the firm indicates, the computing world will join a limited number of mobile phones that are NFC-compatible, acting as 13.56 MHz passive NFC readers and writers that can interrogate tags and capture as well as send data wirelessly when within range of those tags. Microsoft have recently released a Developer Preview build of Windows 8, known as Build 8102, for software and hardware developers to download and begin working with. The tap-to-share application includes software and driver files to enable the use of a plugged- or built-in NFC reader in order to receive or transmit information to or

from another device, such as an NFC tag, an NFC-enabled phone or another NFC-enabled computer running Windows 8. With Windows 7, on the other hand, a user can connect an NFC reader to a computer or laptop, but additional software and a driver, supplied by the reader manufacturer or a third party, are necessary to capture and interpret data transmitted to that reader.

During its Build conference, Microsoft demonstrated the tap-to-share application by means of an NFC-enabled tablet computer loaded with an early version of Windows 8. In response to Microsoft's new OS plans, chip manufacturer NXP Semiconductors has announced that its PN544 NFC radio controller is compatible with the new operating system. In fact, NXP provided the NFC technology used on Windows 8-based tablets distributed at the conference, enabling the computers to not only read and encode NFC RFID tags, but also support peer-to-peer and card-emulation functions specified by NFC standards developed by the NFC Forum.

Last week, RFID tag and inlay manufacturer UPM RFID announced that it has teamed with NFC solutions provider Wireless Sensor Technologies (WST) to provide NFC tags. With this partnership, UPM RFID is providing WST with its NFC tags and inlays that will now be added to WST's NFC readers, software development kits and customization services, including printing and encoding. Although the partnership is not a direct response to the Windows 8 NFC plans, WST notes, it will make it easier for the firm to respond quickly to customers seeking technology solutions built for Windows 8 devices. Wireless Sensor Technologies already provides an NFC app known as GoToTags for computers running Windows 7, enabling users to communicate with an NFC reader plugged into their computer and to use it to read and encode NFC tags. Those in the NFC industry claim that the tap-to-share application signifies that the use of Near Field Communication will grow as NFC support in Windows 8 should spur the new community of developers and end-product manufacturers to create new applications. NFC's use in personal devices which may now include tablets and laptops, as well as mobile phones should enable brick-and-mortar stores to link their products with the Internet.

7. CONCLUSION

NFC is a very short range protocol which is backward compatible with the RFID infrastructure, because of its very short range it is inherently secured from most types of remote attacks. The procedure of establishing communication is very familiar to human's natural way of doing things, you want something to communicate, touch it together. This makes it much more user friendly than the older data transfer methods of searching then establishing a connection. This will make it much less daunting and much more accessible for novice users the whole process feels like devices recognize each other by touch. As the prices of chip manufacturing falls, the likelihood is that NFC-enabled mobile phones will become standard and their applications used in everyday life. As we have experienced with the introduction of smartphones and the thousands of apps that are now available to users, the range and use of NFC applications is bound to increase. The investment in developing the latest mobile technology is proof that the use of mobile phones and our reliance on them in all aspects of our life will continue to grow.

Active NFC devices could have a viable future in commerce, with the beginnings of contactless NFC payments starting to show today with an NFC district in Madrid created and with a proposed number of 60,000 merchants in London to accept NFC for their premises in time for the London 2012 Olympic Games. These pushes towards NFC on the high street are increasing and are pushing the tide towards global acceptance of NFC. Passive NFC tags have great future in advertising because of how small and easy they are to place into a magazine page, a poster in the street or a business card that can be handed out. This will bring advertising into a whole new dimension as the user will be able to 'pull' information from the advertisement if they're interested instead of the traditional 'pushing' of information from the media to the person's senses, as discussed previously.

The fact that NFC is also interoperable with existing smartcard systems should also ensure that this technology would be more easily integrated into existing infrastructures, such as the Transport for London Oyster Card system. As the possibility to store more data on the devices increases, so will the requirements for more complex applications. With any digital transaction, there will always be people who try to manipulate, disrupt or misuse the data that is transmitted and so users will no doubt initially be wary about the security of their personal data that is stored on the NFC devices. Privacy and security will always be a concern for users where personal and sensitive data are involved. We will have to rely on the application developers and handset manufacturers, to ensure that any transaction carried out via a NFC-enabled device is as secure as possible. NFC-enabled devices have great potential. The fact that they are much quicker and easier to learn and use than the normal screen-based interfaces that are currently used on mobile devices, should make them more attractive to those who are less technical and so potentially could reach a wider user

base. Using them for paying for a car parking ticket on exit or for door entry systems in the near future seems almost inevitable.

REFERENCES

[1] NFC Forum. (2011). *About NFC*. Retrieved 04 10, 2011, from NFC Forum: http://www.nfc-forum.org
[2] NFC World. (2011). *About NFC*. Retrieved 04 10, 2011, from NFC World: http://www.nfc-world.com
[3] Conneally, T. (2010, 12 23). *As-NFC-enters-the-mass-market-so-too-should-NFC-security*. Retrieved 04 09, 2011, from Beta News : http://www.betanews.com/
[4] http://public.cenriqueortiz.com/nfc/elements-nfc-jan2009-CEnriqueOrtiz.jpg
[5] *Mobile Phones History*. (2011). Retrieved 04 05, 2011, from Phone History: http://www.phonehistory.co.uk/
[6] Alcatel Lucent. (2011). *Historical Timeline*. Retrieved 04 06, 2011, from Alcatel Lucent: http://www.alcatel-lucent.com/
[7] ISO. (2004, 04 1). *International Standard*. Retrieved 03 24, 2011, from Webstore: http://webstore.iec.ch/preview/info _ isoiec18092%7Bed1.0%7Den.pdf
[8] *NFC In Action*. (2011). Retrieved 04 09, 2011, from NFC Forum: http://www.nfc-forum.org
[9] Clark, S. (2011, 02 27). *Transport for London confirms plans to accept contactless cards in time for olympics*. Retrieved 04 07, 2011, from NearField Communiations World: http://www.nearfieldcommunicationsworld.com/2011/02/27/36204/transport-for-london-confirms-plans-to-accept-contactless-cards-in-time-for-olympics/
[10] Hill, J. (2011, 04 04). *The question of security with nfc based payments*. Retrieved 04 08, 2011, from Gadgetell: http://www.gadgetell.com/tech/comment/the-question-of-security-with-nfc-based-payments/
[11] http://www.google.com/wallet/