REPORT:

NEAR FIELD COMMUNICATION (NFC)

PAKISTAN TELECOM AUTHORITY

NOV 2010

Contents

Terms, Abbreviations, and List of Acronyms

NFC	***Near Field Communication***
ISO	***International Organization for Standardization***
IEC	***International Electro-Technical Commission***
RFID	***Radio Frequency Identification***
RF	***Radio Frequency***
ASK	***Amplitude shift keying***
IrDA	***Infrared Data Association***
ISM	***Industrial Scientific and Medical***
ACMA	***Australian Communications and Media Authority's***
ofcom	***UK Based Communications Regulator***
iDA	***Singapore Based Regulator***
FCC	***Federal Communication Commission (USA)***
CRTC	***Canadian Radio-Television and Telecommunication Commission***
FeliCa	***Contactless RFID smart card system by Sony in Japan***
IC	***Integrated Circuit***
CAO	***Club Airport Premium***
IEEE	***International Electrical and Electronics Engineering***
SIG	***Special Interest Group***
NFCIP	***NFC Interface and Protocol***
NDEF	***NFC Data Exchange Format***
MIME	***Multipurpose Internet Mail Extensions***
GSMA	***GSM Association***
StoLPaN	***Store Logistics and Payments with NFC***
SCP	***Smart Card Platform***
ETSI	***European Telecommunications Standards Institute***
EMV	***Europay, MasterCard and VISA***

Executive Summary

This comprehensive study paper prepared by Strategy & Development Division highlights the major areas of NFCs.

NFC is dual Technology which comes in Short Range Devices (SRDs) and in near future is likely to replace Bluetooth and other SRDs technology for inherent advantages in power battery consumption, to avoid the complicated configuration process and to reduce the set up time. The Bluetooth technology evolved during this decade has been in use worldwide; however certain disadvantages of Bluetooth have been in focus of global Research and Development centers.

If we go through the previous technologies then we find that the Infrared technology (Line of sight technology) was replaced by Bluetooth and RFID technology but now the new technology NFC replace the RFID and Bluetooth due to some deficiencies in them which we discussed in this paper.

The technology development locations around the globe such as North America, Japan, Korea, China, Sweden, Germany etc are actively involved in designing efficient NFCs which will be available in the next few years. They promote the Near Field Communication Applications across the globe which is in related to Medical, Security and Identification, Electronic Payments, Electronic cards, Electronic Keys Etc. In Tier-1 countries absorption of NFCs in developed market is currently seen and it is expected that the demanded price devices and applications will make NFCs available to relatively developing and less developed countries.

This is observed that markets like Pakistan are reluctant in change of system technologies. New products introduced do not actively replace the existent technology. Electronic affordability index of a country has a key role in replacement of existing technologies, systems and devices.

In this consultation document we discuss the NFC in detail regarding their Specifications, Uses and Applications of NFCs, Standardization bodies and Industrial Projects, Security key aspects and their Solutions and Recommendations.

NFC is the advance technology of Bluetooth and RFID; this technology can be introduced by the mutual concentrations of Telecom vendors and Operators as the Bluetooth came.

So in this regard the Pakistan Regulatory body would have to pursue for NFC and initialize the frequency of 13.56 MHz in Industrial, Scientific and Medical (ISM) band of Pakistan so that NFC can be implement. Currently the different international regulatory bodies (ACMA, OFCOM, FCC, IDA etc) have recommended NFCs and its applications. This technology operates in the frequency of 13.56 MHz which is in globally available unlicensed radio frequency ISM band.

1. Near Field Communication (NFC)

NFC is a short-range high frequency wireless communication technology which enables the exchange of data between devices over about a 10 centimeter (around 4 inches) distance. The technology is a simple extension of the International Organization for Standardization/ International Electro-Technical Commission (ISO/IEC) 14443 proximity-card standard (proximity card, RFID) that combines the interface of a smartcard and a reader into a single device. An NFC device can communicate with both existing ISO/IEC 14443 smartcards and readers, as well as with other NFC devices, and is thereby compatible with existing contactless infrastructure already in use for public transportation and payment. NFC is primarily aimed at usage in mobile phones.

From the techno-economic viewpoint, the advantages of NFC over alternative wireless communication technologies such as Bluetooth and Infrared Data Association (IrDA) are its lower price, lower power consumption and better immunity to eavesdropping. NFC can potentially improve the usability of many health monitoring devices.

2. Essential Specifications:

- Like ISO/IEC 14443, NFC communicates via magnetic field induction, where two loop antennas are located within each other's near field, effectively forming an air-core transformer. It operates within the globally available and unlicensed radio frequency ISM band of 13.56 MHz, with a bandwidth of 14 KHz.
- Another of its major appeals is that it is both a 'read' and 'write' technology, thus allowing for the transfer and storage of data between each of the respective devices.
- Working distance with compact standard antennas: up to 20 cm
- Supported data rates: 106, 212, 424 or 848 Kbit/s

- Some NFC manufacturers and suppliers are Mannings, Promobox, Touch Tag, Card xx, Sag, NXP etc.

Source: NFC India, Reference No 18

2.1 Modes of Communication in NFC

There are two modes:

- **Passive Communication Mode**: The Initiator device provides a carrier field and the target device answers by modulating existing field. In this mode, the Target device may draw its operating power from the Initiator-provided electromagnetic field, thus making the Target device a transponder.

- **Active Communication Mode**: Both Initiator and Target device communicate by alternately generating their own field. A device deactivates its RF field while it is waiting for data. In this mode, both devices typically need to have a power supply.

Baud Rate	Active device	Passive device
424 kbps	**Manchester, 10% ASK**	**Manchester, 10% ASK**
212 kbps	**Manchester, 10% ASK**	**Manchester, 10% ASK**
106 kbps	**Modified Miller, 100% ASK**	**Manchester, 10% ASK**

Source: NFC Specifications, Reference No 1

When two devices communicate three different configurations are possible. These are described in Table as:

Table: Communication Configurations

Device A	Device B	Description
Active	Active	When a device sends data it generates an RF field. When waiting for data a device does not generate an RF field. Thus, the RF field is alternately generated by Device A and Device B
Active	Passive	The RF field is generated by Device A only
Passive	Active	The RF field is generated by Device B only

Source: Security in NFC, Reference No 2

These above configurations are important because the way data is transmitted depends on whether the transmitting device is in active or passive mode.

In active mode the data is sent using amplitude shift keying (ASK). This means the base RF signal (13.56 MHz) is modulated with the data according to a coding scheme. If the baud rate is 106 Kbits/s, the coding scheme is the so-called modified Miller coding. If the baud rate is greater than 106 Kbits/s the Manchester coding scheme is applied. In both coding schemes a single data bit is sent in a fixed time slot. This time slot is divided into two halves, called half bits. In Miller coding a zero is encoded with a pause in the first half bit and no pause in the second half bit. A one is encoded with no pause in the first bit, but a pause in the second half bit. In the modified Miller coding some additional rules are applied on the coding of zeros. In the case of a one followed by a zero, two subsequent half bits would have a pause. Modified Miller coding avoids this by encoding a zero, which directly follows a one with two half bits with no pause.

In the Manchester coding the situation is nearly the same, but instead of having a pause in the first or second half bit, the whole half bit is either a pause or modulated. Besides the coding scheme also the strength of the modulation depends on the baud rate.

For 106 Kbit/s 100% modulation is used. This means that in a pause the RF signal is actually zero. No RF signal is sent in a pause. For baud rates greater than 106 Kbits/s 10% modulation ratios is used. According to the definition of this modulation ratio, this means that in a pause the RF signal is not zero, but it is about 82% of the level of a non paused signal. This difference in the modulation strength is very important from a security point of view as we will describe later on in the security analysis.

In passive mode the data is sent using a weak load modulation. The data is always encoded using Manchester coding with a modulation of 10%. For 106 Kbits/s a subcarrier frequency is used for the modulation, for baud rates greater than 106 Kbits/s the base RF signal at 13.56 MHz is modulated.

Additionally to the active and passive mode, there are two different roles a device can play in NFC communication. NFC is based on a message and reply concept. This means one device sends a message to another device B and device B sends back a reply. It is not possible for device B to send any data to device A without first receiving some message from device A, to which it could reply. The role of the device A which starts the data exchange is called initiator, the role of the other device is called target. The following Table lists all possible combinations of this role with respect to the active or passive mode. Only the combination Initiator and Passive is not possible.

Possible Combinations Active/Passive with Initiator/Target

	Initiator	Target
Active	Possible	Possible
Passive	Not Possible	Possible

Source: Security in NFC, Reference No 2

Furthermore it should be mentioned that NFC communication is not limited to a pair of two devices. In fact one initiator device can talk to multiple target devices. In this case all target devices are enabled at the same time, but before sending a message, the initiator device must select a receiving device. The message must then be ignored by all non selected target devices. Only the selected target device is allowed to answer to the received data. Therefore, it is not possible to send data to more than one device at the same time (i.e. broadcasting messages are not possible).

- NFC devices are able to receive and transmit data at the same time. Thus, they can check the radio frequency field and detect a collision if the received signal does not match with the transmitted signal.

2.2 NFC Tag types

There are four basic tag types that have been defined. These are given designations 1 to 4 and each has a different format and capacity. These NFC tag types format are based on ISO 14443 (Types A and B which is the international standard for contact-less smartcards) and Sony FeliCa which conforms to ISO 18092 (the passive communication mode, standard).
The advantage of keeping the NFC tags as simple as possible is that they may be deemed to be disposable in many instances, often embedded in posters that may only have a short life, etc.

The different NFC tag type definitions are as follows:

Tag-1 Type:
The Tag 1 Type is based on the ISO14443A standard. These NFC tags are read and re-write capable and users can configure the tag to become read-only.
Memory availability is 96 bytes which is more than sufficient to store a website URL or other small amount of data. However the memory size is expandable up to 2 kbyte. The communication speed of this NFC tag is 106 kbit/s. As a result of its simplicity this tag type is cost effective and ideal for many NFC applications.

Tag-2 Type:
The NFC Tag 2 Type is also based on ISO14443A. These NFC tags are read and re-write capable and users can configure the tag to become read-only. The basic memory size of this tag type is only 48 bytes although this can be expanded to 2 kbyte. Again the communication speed is 106 Kbit/s.

Tag-3 Type:
The NFC Tag 3 Type is based on the Sony FeliCa system. It currently has a 2 Kbyte memory capacity and the data communications speed is 212 Kbit/s. accordingly this NFC tag type is more applicable for more complex applications, although there is a higher cost per tag.

Tag-4 Type:
The NFC Tag 4 Type is defined to be compatible with ISO14443A and B standards. These NFC tags are pre-configured at manufacture and they can be read / re-writable, or read-only. The memory capacity can be up to 32 Kbytes and the communication speed is between 106 Kbit/s and 424 Kbit/s.

From the definitions of the different NFC tag types, it can be seen that type 1 and 2 tags are very different to type 3 and 4 tags, having different memory capacity and makeup. Accordingly it is expected that there is likely to be very little overlap in their applications.
Type 1 and type 2 tags are dual state and may be either read/write or read-only. Type 3 and Type 4 tags are read-only, data being entered at manufacture or using a special tag writer.

Passive tag Operation:
The Passive NFC tag is a passive device with no power of its own. Accordingly when one is used, the users touch an NFC enabled device onto the tag. A small amount of power is taken by the NFC tag from the reader/writer to power the tag electronics. The tag is then enabled to transfer a small amount of information to the reader/writer.
The data stored in the tag memory is transferred to the NFC enabled device. Although normally only a small amount of data, this may be used to direct the device to a website
URL; it may be a small amount of text, or other data.

NFC tag design and manufacture
There are many design and manufacturing considerations to be taken into account for NFC tags. They are intended to be manufactured for very low cost in very large quantities, while maintaining their performance. There are a number of key performance parameters and elements that need to be considered when designing an NFC tag.

Read speed: This issue is important because it is necessary for the NFC tag to be able to pass all its data over while the two NFC devices are within range. If the NFC tag can only transfer data at a slow rate then there is a real danger that all the data may not be transferred in time resulting in a poor level of reliability. In turn this will affect the user and the user, who not understanding the technology will easily be turned off from using the system if they have to keep re-trying to successfully transfer the data. NFC tag type 1 allows all the data to be transferred in one block which enables the read performance of the tag to be maintained.

Die size: The die size is of particular importance in the design of an NFC tag. A smaller die, results in lower cost and also the in the NFC tag being less obtrusive - an important factor for tags used in posters, etc. Smaller memory sizes naturally lend themselves to smaller die sizes.

Unit price: The unit price of the NFC is a very important factor in their design as many NFC tags will be aimed for very low cost applications such as smart posters. Here cost is of great importance. The cost of the tag is influenced by a number of factors. These include factors such as the memory size and general IC complexity resulting from additional features that need to be included; by keeping the memory and features as simple as possible the cost can be kept down.

With manufacture of NFC tags likely to run into billions when the system fully takes off, the design of tags will need to be undertaken very carefully so that the correct balance of cost and performance can be obtained.

3. NFC Uses and Applications

NFC the perfect storm to put an end to CASH:

It is quite interesting to have a discussion not just about payments, but around modality and the emergence of strong mobile payments methodology and practices. We already know that checks/ are in terminal decline, but when you bring up the 'end of cash' this gets a great deal of emotive responses or general disbelief that this is possible or probable. It is becoming quite clear, however, that regardless of the emotion and habitual systemic behavior that there is an number of issues that are combining to create a critical decision point for governments, regulators and the banking community to get *actively* behind the removal of cash from the system.

Net Social Cost:

Cash costs society comparatively significantly more than alternative payments methods such as debit cards. Leo van Hove, Associate Professor of Economics at the Free University of Brussels, says that in Belgium 10.24 Euro is the threshold where cash starts to lose it's efficiency due to marginal costs, and in Netherlands this is about 11 Euro. Additional social costs beyond distribution, including money laundering, gambling, crime, etc that make physical money a net negative in the social impact picture under most scenarios.

Base Materials and Production

An average US 1 Penny coin costs 1.67 cents to manufacture, and the Dime (5 cent piece) costs 7.7 cents to manufacture. So it is clear that coins in general are becoming untenable as raw materials costs for copper, silver, gold, etc climb yet further. Carol Realini projects that the future need for physical cash into the Indian economy would take more paper than can be

produced from all the trees in the world if based on real physical currency. With an increasing focus on carbon cost of production, then surely cash itself is a massively expensive proposition for society and is no longer an efficient mechanism for governments. Banks may be holding on to cash because their retail businesses are still largely based on physical cash distribution, but the reality is this is a false economy for society as a whole and is certainly not responsible as we move towards a greener future.

Not mathematically efficient

A Blog Post from the Freakonomics gang that suggests that the correct denominations for coins should be 3-cents, 11-cents and 37-cents based on correlations between pricing, spend, coin production, distribution, etc. Another post suggests that we need 5-cent, 18-cent and half-dollar combination.

By one estimate, $10.5 billion in coins just sits around in people's homes gathering dust... Alan Burdick, Discover - The Physics of Pocket Change

Mobile Payments and contact-less Debit Cards

There's been a lot of chatter about mobile payments, the NFC integrated iPhone, M-PESA, G-Cash, PayPal and so forth in the blogosphere lately. It is clear there is a lot of anticipation of this potential, but there remain some challenges. Ubiquity is going to be challenging because just like with physical cash and currency, competing standards may actual work against adoption. Interoperability between payments networks, between e-Cash and physical cash, etc will be a challenge too.

Nobuhiko Sugiura, a Special Research Fellow of Japan's Financial Services Authority, and the Associate Dean of Chuo University Business School highlights the fact that once the regulators got behind e-Money in Japan then it's success was rapid. Just in the last 3 years use of e-Money has increased 300% now to be one of the most frequented personal payment mechanisms in Japan. In fact, one third of Japanese, according to Sugiura-san are already e-Money users. He cited some other great drivers behind e-Money's success in Japan, which translate as equally well to countries outside of Japan, namely:

- Japanese banks have no interest in micro-payments because of the relatively cost base.
- Convenience stores favor e-Money so that they can reduce their cash float.
- The unwritten law in Japan is that refunds are "prohibited in principle", because the Japanese governments want to replace Physical cash with e-Money as quickly as possible.

In the UK, 43 per cent of retail payments are done by debit card and 23 per cent by credit card. Cash still makes up 32 per cent of these payments, but as a percentage of the whole, it continues to reduce. This is a trend throughout the EU and much of the Western world.

So we can conclude given all of the above, it must just be pure momentum in the system as to why we are still using cash. In terms of cries from industry that "cash is back" it would appear that this sentiment should be discouraged at all costs. If you want to encourage savings then promote debit card and e-Money usage, but physical cash is bad for the system all round.

NFC technology is currently mainly aimed at being used with mobile phones. There are three main use cases for NFC:

- **Card emulation**: the NFC device behaves like an existing contactless card
- **Reader mode**: the NFC device is active and read a passive RFID tag, for example for interactive advertising.
- **P2P mode**: Two NFC devices are communicating together and exchanging information.

When it comes to mobile payments there's a lot of talk and activity vis-à-vis P2P & remote purchasing. The biggest potential is the POS market. It is the best-served payments market with large number of terminal and involving several cards of all banked and non-banked consumers. Some suggest that the way-forward for mobile payments at the POS can be none other than the emerging near field communication technology.

It is impossible to give a complete picture of NFC applications as NFC is just an interface. Plenty of applications are possible, such as:

- Mobile ticketing in public transport — an extension of the existing contactless infrastructure. Such as Mobile Phone Boarding Pass.
- Mobile payment — the device acts as a debit/ credit payment card.
- Smart poster — the mobile phone is used to read RFID tags on outdoor billboards in order to get info on the move.
- Bluetooth pairing — in the future pairing of Bluetooth 2.1 devices with NFC support will be as easy as bringing them close together and accepting the pairing. The process of activating Bluetooth on both sides, searching, waiting, pairing and authorization will be replaced by a simple "touch" of the mobile phones.

Other applications in the future could include:

- Electronic ticketing —concert/event tickets, and others
- Electronic money
- Travel cards
- Identity documents
- Mobile commerce
- Electronic keys — car keys, house/office keys, hotel room keys, etc.
- NFC can be used to configure and initiate other wireless network connections such as Bluetooth, Wi-Fi or Ultra-wideband.
- Room Accessories Automation
- Identification and Authentication
- Parking Automation and Toll Collection
- Time attendance etc etc.

3.1 Obstacles for NFC deployment

- Card issuers and carriers will argue on sharing cost to enable secure storage of card data on phones. However, the banking industry may by-pass it by offering solutions through SD Memory cards, External Tags or burning in software through specialized tool-kits. Applicable fees could be one-time, yearly rental, or a fraction of the transaction. We have to realize that NFC will be replacing an existing card-swipe process. Some issues which need to be resolved are:
- Price of adding NFC to an old type cell phone
- Installing or upgrading reader conventional POS terminals.
- Developing confidence in the minds of the users to use their cell phones for mobile-transaction via NFC instead of conventional proven methods.

- Handheld phones are used carelessly and one may worry what if such a smart device without necessary safeguard land into someone else hand, who is also capable of breaking the code.

3.2 NFC-enabled mobile phones – the future of the check-in process?

Source: Future of NFC, Reference No 3

Beunardeau: "We have proven that we can use NFC for real operations of aircraft as people were successfully boarding planes using the technology."

The technology is still in its relative infancy – at least within the aviation sector – pilot schemes have already been undertaken to put the viability of the technology to the test.

3.3 NFC in action

Last year, Air France, Amadeus and IER partnered with Nice Côte d'Azur Airport in one of the industry's largest NFC pilot schemes. Over a six-month period, members of the airport's Club Airport Premier (CAP) passenger programme and the airline's frequent flyer programme travelling on the route between Nice and Paris Orly piloted Pass and Fly – an NFC-based boarding pass.

The idea of the project was to establish whether passenger recognition, the crediting of CAP points and aircraft boarding could be simplified through the use of the wireless technology. To enable the project, Amadeus developed the NFC application for mobile phones, while the company worked with its partners to develop the departure control system and the NFC readers. Once the infrastructure was in place, the NFC-enabled mobile phones could interact directly with the NFC readers.

"We decided to try to see how this technology works and we wanted to see whether using NFC technology for a real flight was possible," said Yannick Beunardeau, director airport solutions, Amadeus. "What we have since proven is that we can use NFC for real operations of aircraft as people were successfully boarding planes using the technology. The airline, the airport and the passengers all appreciated the way that the technology was working. For the passenger, there were many benefits, mostly the fact that they didn't even need to print their boarding pass. Normally, they had to show their boarding pass and their card to get the fast track, and another to collect the frequent flyer points. Instead, using NFC technology enabled all of these processes to be complete in one transaction in a matter of milliseconds."

Source: NFC in Action, Reference No 3

While the main idea of the project was to establish the potential of NFC-based boarding passes, Beunardeau explained that the technology can provide further benefits. These include implementing NFC-based payment systems and using the technology to allow access to restricted areas of the airport, as well as using NFC to provide the airport with information on passenger flows between two specified points.

3.4 Future challenges

Of course, each of these processes would require the passenger or member of staff in question to have access to an NFC-enabled mobile phone, but with such handsets yet to be made widely available, the widespread implementation of the technology appears to face a major hurdle.
However, mobile phone manufacturers – namely Nokia and Apple – have recently vowed to integrate the technology into their future handsets, with NFC-enabled smart phones expected to be more readily available as early as next year. Furthermore, Beunardeau explained that Amadeus has designed a chip that can be added to the phone in the form of a sticker, which will enable the handset to be used as an NFC device.

Another issue that also needs to be addressed is that of cost. Beunardeau said: "As NFC readers use an existing reader with some modifications, it isn't too expensive to implement and I wouldn't say that it is out of range because of cost. We have to remember, also, that this could provide a permanent solution."

NFC to health monitoring applications as an easy to use, low-power and low-cost wireless interface for medical sensors and instruments such as blood pressure monitors, blood glucose monitors, heart rate monitors and personal weight scales, and facilitating the use of mobile terminals as a patient's user interface, as well as a gateway to the backend system.

4. RFID vs. NFC

RFID (Radio Frequency Identification) is a tagging technology that is gaining widespread attention due to the great number of advantages that it offers compared to the current tagging technologies being used today; like barcodes. Near Field Communication, or more commonly known as NFC, is a subset of RFID that limits the range of communication to within 10 centimeters or 4 inches.

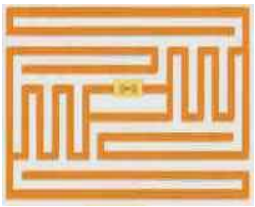
RFID uses radio frequency waves that are either passive, active, or a combination of both. Active RFID tags have a power source that helps extend their range even further while passive devices rely on the energy that it receives from the interrogating device to send its own information. Among the advantages of RFID is the very small size of the tag that made it possible to be used with small products or to be hidden away neatly. Another excellent advantage is that it doesn't need a direct line of sight for the information to be read. This is very desirable in baggage tracking application where speed is very essential.

RF waves are used to transmit information across very long distances, and RFID is no different. RFID can possibly have a lot of simple applications by simply attaching a passive RFID sticker to phone, externally, and prove useful for things like anti-theft, or tracking an employee inside a building, or a patient or a doctor within a hospital.
The RF waves can reach very long distances especially when powered. This kind of range is very desirable in certain applications like animal tracking where the animal being tracked might move a couple of kilometers. But this type of range is not desirable in applications like cash cards or passports. Malicious people can receive your information and clone it into another tag and use it for themselves. This is where NFC comes in.

	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~O.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

Source: RFID and NFC, IrDa, Bluetooth, Reference No 6

Objects that are tagged with NFC are usually passive because it does not require that much range. Some have even employed shielding to further reduce the chance of other people being able to read the information. The shielding became necessary when it was discovered that even non-powered tags can still be read over 10 meters away with specialized equipment. Currently, some mobile phones are being equipped with NFC so that they can be used as a cash card of sorts since almost all people carry mobile phones anyway.



Source: RFID and NFC, Reference No 5

NFC is more secure than RFIDs, but shorter-range.
NFC is being standardized through slow but, maybe watchful, process and tied into many business modelswith operators, especially GSM. We need to ensure that WiMax and EVDO operators also go along. Other than ePayment applications the security complexity may have been over emphasized.
RFID has longer range but is a bit less secure.
A wavering question is how NFC links in to handset user interface and applications.

Summary:
1. NFC is just an extension to RFID technology.
2. RFID is capable of accepting and transmitting beyond a few meters while NFC is restricted to within 4 inches.
3. RFID has a wide range of uses while NFC is usually used in cases where security is needed.
4. Some mobile phones are equipped with NFC.

5. NFC vs. Bluetooth

	NFC	Bluetooth V2.1	Bluetooth V4.0
RFID compatible	ISO 18000-3	Active	Active
Standardization body	ISO/IEC	Bluetooth SIG	Bluetooth SIG
Network Standard	ISO 13157 etc.	IEEE 802.15.1	IEEE 802.15.1
Network Type	Point-to-point	WPAN	WPAN
Cryptography	not with RFID	Available	Available
Range	< 0.2 m	~10 m (class 2)	~1 m (class 3)
Frequency	13.56 MHz	2.4-2.5 GHz	2.4-2.5 GHz
Bit rate	424 kbit/s	2.1 Mbit/s	~200 kbit/s
Set-up time	< 0.1 s	< 6 s	< 1 s
Power consumption	653mw(Reader/writer)	2.5mw(both)	1mw(both)

Source: NFC Vs Bluetooth, Reference No 1

NFC and Bluetooth are both short-range communication technologies which have recently been integrated into mobile phones. To avoid the complicated configuration process, NFC can be used for the set-up of wireless technologies, such as Bluetooth.

The earlier advantage of NFC over Bluetooth with the shorter set-up time is still valid with standard Bluetooth protocol stack, but no more with Bluetooth V4.0 low energy protocol stack.

With NFC, instead of performing manual configurations to identify devices, the connection between two NFC devices is established at once (faster than a tenth of a second). The maximum

data transfer rate of NFC (424 Kbit/s) is slower than Bluetooth V2.1 (2.1 Mbit/s). With less than 20 cm, NFC has a shorter range, which provides a limitation of threat. That mostly makes NFC suitable for crowded areas when correlating a signal with its transmitting physical device (and by extension, its user) becomes difficult.

In contrast to Bluetooth, NFC is compatible with existing passive RFID (13.56 MHz ISO/IEC 18000-3) infrastructures. NFC requires comparably low power as Bluetooth V4.0 low energy protocol. When NFC alternatively works with one of the devices is not powered (e.g. on a phone that may be turned off, a contactless smart credit card, a smart poster, etc.), then the NFC power consumption exceeds the Bluetooth V4.0 Low Energy power consumption level due to required illumination of then passive tag.

6. Standardization bodies and industry projects

6.1 Standards

NFC was approved as an ISO/IEC standard on December 8, 2003 and later as an ECMA standard.
NFC is an open platform technology standardized in ECMA-340 and ISO/IEC 18092. These standards specify the modulation schemes, coding, transfer speeds and frame format of the RF interface of NFC devices, as well as initialization schemes and conditions required for data collision-control during initialization-for both passive and active NFC modes. Furthermore, they also define the transport protocol, including protocol activation and data-exchange methods. Air interface for NFC is standardized in: ISO/IEC 18092 / ECMA-340: Near Field Communication Interface and Protocol-1 (NFCIP-1) ISO/IEC 21481 / ECMA-352: Near Field Communication Interface and Protocol-2 (NFCIP-2).

NFC incorporates a variety of pre-existing standards including ISO/IEC 14443 both Type A (normal) and Type B (banking/short range), and FeliCa. NFC enabled phones thus show basic interoperability with the preexisting reader infrastructure. Especially in "card emulation mode" a NFC device should at least transmit a unique ID number to a pre-existing reader.
In addition, NFC Forum has defined a common data format called NDEF, which can be used to store and transport different kinds of items, ranging from any MIME-typed object to ultra-short RTD-documents, such as URLs.

NDEF is conceptually very similar to MIME. It is a dense binary format of so-called "records", in which each record can hold a different type of object. By convention, the type of the first record defines the context of the entire message.

6.2 GSMA

The GSM Association (GSMA) is the global trade association representing 700 mobile phone operators across 218 countries of the world.

They have launched two initiatives:

- The **Mobile NFC initiative**: fourteen mobile network operators, who together represent 40% of the global mobile market, back NFC and are working together to develop NFC applications. They are Bouygues Télécom, China Mobile, AT&T, KPN, Mobilkom Austria, Orange,

SFR, SKTelecom, TelefonicaMóviles spaña, Telenor, TeliaSonera, Telecom Italia Mobile (TIM), Vodafone.

- On 13 February 2007, they published a white paper on NFC to give the point of view of mobile operators on the NFC ecosystem.
- The **Pay buy mobile initiative** seeks to define a common global approach to using Near Field Communications (NFC) technology to link mobile devices with payment and contactless systems. To date, 30 mobile operators have joined this initiative.

6.3 StoLPaN:

StoLPaN ('Store Logistics and Payment with NFC') is a pan-European consortium supported by the European Commission's Information Society Technologies program. StoLPaN will examine the as yet untapped potential for bringing together the new kind of local wireless interface, NFC and mobile communication.

6.4 NFC Forum

The NFC Forum is a non-profit industry association announced on March 18, 2004 by NXP Semiconductors, Sony and Nokia to advance the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs. The NFC Forum promotes implementation and standardization of NFC technology to ensure interoperability between devices and services. In September 2008, there were over 150 members of the NFC Forum.

6.5 Other standardization bodies

Other standardization bodies that are involved in NFC include:

- ETSI / SCP (Smart Card Platform) to specify the interface between the SIM card and the NFC chipset.
- Global Platform to specify a multi-application architecture of the secure element.
- EMVCo for the impacts on the EMV payment applications.

7. Security aspects

Although the communication range of NFC is limited to a few centimeters, NFC alone does not ensure secure communications. In 2006, Ernst Haselsteiner and Klemens Breitfuß described some possible types of attacks.

NFC offers no protection against eavesdropping and is also vulnerable to data modifications. Applications have to use higher-layercryptographic protocols (e.g., SSL) to establish a secure channel.

7.1 Eavesdropping

Because NFC is a wireless communication interface it is obvious that eavesdropping is an important issue. When two devices communicate via NFC they use RF waves to talk to each other. An attacker can of course use an antenna to also receive the transmitted signals. Either by experimenting or by literature research the attacker can have the required knowledge on how to extract the transmitted data out of the received RF signal. Also the equipment required to receive the RF signal as well as the equipment to decode the RF signal must be assumed to be available to an attacker as there is no special equipment necessary.

The NFC communication is usually done between two devices in close proximity. This means they are not more than 10 cm (typically less) away from each other. The main question is how close an attacker needs to be to be able to retrieve a usable RF signal. Unfortunately, there is no correct answer to this question. The reason for that is the huge number of parameters which determine the answer. For example the distance depends on the following parameters, and there are many more.

- RF filed characteristic of the given sender device (i.e. antenna geometry, shielding effect of the case, the PCB, the environment)
- Characteristic of the attacker's antenna (i.e. antenna geometry, possibility to change the position in all 3 dimensions)
- Quality of the attacker's receiver
- Quality of the attacker's RF signal decoder
- Setup of the location where the attack is performed (e.g. barriers like walls or metal, noise floor level)
- Power sent out by the NFC device.

Therefore any exact number given would only be valid for a certain set of the above given parameters and cannot be used to derive general security guidelines.
Additionally, it is of major importance in which mode the sender of the data is operating. This means whether the sender is generating it's own RF field (active mode) or whether the sender is using the RF field generated by another device (passive mode). Both cases use a different way of transmitting the data and it is much harder to eavesdrop on devices sending data in passive mode.

In order to not leave the reader without any idea on how big the eavesdropping distances are, we give the following numbers, which as stated above are not valid in general at all, but can only serve to give a rough idea about these distances.
When a device is sending data in active mode, eavesdropping can be done up to a distance of about 10 m, whereas when the sending device is in passive mode, this distance is significantly reduced to about 1 m.

7.2 Data Corruption

Instead of just listening an attacker can also try to modify the data which is transmitted via the NFC interface. In the simplest case the attacker just wants to disturb the communication such that the receiver is not able to understand the data sent by the other device.

Data corruption can be achieved by transmitting valid frequencies of the data spectrum at a correct time. The correct time can be calculated if the attacker has a good understanding of the used modulation scheme and coding. This attack is not too complicated, but it does not allow the attacker to manipulate the actual data. It is basically a Denial of Service attack.

7.3 Data Modification

In data modification the attacker wants the receiving device to actually receive some valid, but manipulated data. This is very different from just data corruption.

The feasibility of this attack highly depends on the applied strength of the amplitude modulation. This is because the decoding of the signal is different for 100% and 10% modulation.

In 100% modulation the decoder basically checks the two half bits for RF signal on (no pause) or RF signal off (pause). In order to make the decoder understand a one as a zero or vice versa, the attacker must do two things. First, a pause in the modulation must be filled up with the carrier frequency. This is feasible. But, secondly, the attacker must generate a pause of the RF signal, which is received by the legitimate receiver. This means the attacker must send out some RF signal such that this signal perfectly overlaps with the original signal at the receiver's antenna to give a zero signal at the receiver. This is practically impossible. However, due to the modified Miller coding in the case of two subsequent ones, the attacker can change the second one into a zero, by filling the pause which encodes the second one. The decoder would then see no pause in the second bit and would decode this as a correct zero, because it is preceded by a one. In 100% modulation an attacker can therefore never change a bit of value 0 to a bit of value 1, but an attacker can change a bit of value 1 to a bit of value 0, in case this bit is preceded by a bit of value 1 (i.e. with a probability of 0.5).

In 10% modulation the decoder measures both signal levels (82% and Full) and compares them. In case they are in the correct range the signal is valid and gets decoded. An attacker could try to add a signal to the 82% signal, such that the 82% signal appears as the Full signal and the actual Full signal becomes the 82% signal. This way the decode would decode a valid bit of the opposite value of the bit sent by the correct sender. Whether the attack is feasible depends a lot on the dynamic input range of the receiver. It is very likely that the much higher signal level of the modified signal would exceed the possible input range, but for certain situations this cannot be ruled out completely.

The conclusion is that for the modified Miller encoding with 100% ASK this attack is feasible for certain bits and impossible for other bits, but for Manchester coding with 10% ASK this attack is feasible on all bits.

7.4 Data Insertion

This means that the attacker inserts messages into the data exchange between two devices. But this is only possible, in case the answering device needs a very long time to answer. The attacker could then send his data earlier than the valid receiver. The insertion will be successful, only, if the inserted data can be transmitted, before the original device starts with the answer. If both data streams overlap, the data will be corrupted.

7.5 Man-in-the-Middle-Attack

In the classical Man-in-the-Middle Attack, two parties which want to talk to each other, called Alice and Bob, are tricked into a three party conversation by an attacker Eve. This is shown in Figure 1.

Figure 1 Man-in-the-Middle Setup

Source: Threats in NFC, Reference No 2

Alice and Bob must not be aware of the fact that they are not talking to each other, but that they are both sending and receiving data from Eve. Such a setup is the classical threat in unauthenticated key agreement protocols like Diffie-Hellmann protocol. Alice and Bob want to agree on a secret key, which they then use for a secure channel. However, as Eve is in the middle, it is possible for Eve to establish a key with Alice and another key with Bob. When Alice and Bob later use their key to secure data, Eve is able to eavesdrop on the communication and also to manipulate data being transferred.

How would that work when the link between Alice and Bob is an NFC link?

Assuming that Alice uses active mode and Bob would be in passive mode, we have the following situation. Alice generates the RF field and sends data to Bob. In case Eve is close enough, she can eavesdrop the data sent by Alice. Additionally she must actively disturb the transmission of Alice to make sure that Bob doesn't receive the data. This is possible for Eve, but this can also be detected by Alice. In case Alice detects the disturbance, Alice can stop the key agreement protocol. Let's assume Alice does not check for active disturbance and so the protocol can continue. In the next step Eve needs to send data to Bob. That's already a problem, because the RF field generated by Alice is still there, so Eve has to generate a second RF field. This however, causes two RF fields to be active at the same time. It is practically impossible to perfectly align these two RF fields. Thus, it is practically impossible for Bob to understand data sent by Eve. Because of this and the possibility of Alice to detect the attack much earlier we conclude that in this setup a Man-in-the-Middle attacks is practically impossible.

The only other possible setup is that Alice uses active mode and Bob uses active mode, too. In this case Alice sends some data to Bob. Eve can list and Eve again must disturb the transmission of Alice to make sure that Bob does not receive the data. At this point Alice could already detect the disturbance done by Eve and stop the protocol. Again, let us assume that Alice does not do this check and the protocol continues. In the next step Eve would need to send data to Bob. At first sight this looks better now, because of the active-active communication Alice has turned off the RF field. Now Eve turns on the RF field and can send the data. The problem here now is that also Alice is listening as she is expecting an answer from Bob. Instead she will receive the data sent by Eve and can again detect a problem in the protocol and stop the protocol. It is impossible in this setup for Eve to send data either to Alice or Bob and making sure that this data is not received by Bob or Alice, respectively.

We claim that due to the above given reasons it is practically infeasible to mount a Man-in-the-Middle attack in a real-word scenario.

8. Solutions and Recommendations

8.1 Eavesdropping

As described in section 7.1, NFC by itself cannot protect against eavesdropping. It is important to note that data transmitted in passive mode is significantly harder to be eavesdropped on, but just using the passive mode is probably not sufficient for most applications which transmit sensitive data. The only real solution to eavesdropping is to establish a secure channel as outlined in section 8.6.

8.2 Data Corruption

NFC devices can counter this attack because they can check the RF field, while they are transmitting data. If NFC devices do this, it will be able to detect the attack. The power which is needed to corrupt the data is significantly bigger, than the power which can be detected by the NFC device. Thus, every such attack should be detectable.

8.3 Data Modification

Protection against data modification can be achieved in various ways.

By using 106k Baud in active mode it gets impossible for an attacker to modify all the data transmitted via the RF link as described in section 7.3. This means that for both directions active mode would be needed to protect against data modification. While this is possible, this has the major drawback, that this mode is most vulnerable to eavesdropping. Also, the protection against modification is not perfect, as even at 106k Baud some bits can be modified. The two other options might therefore be preferred.

NFC devices can check the RF field while sending. This means the sending device could continuously check for such an attack and could stop the data transmission when an attack is detected.

The third and probably best solution would be a secure channel as described in next sections.

8.4 Data Insertion

There are three possible countermeasures. One is that the answering device answers with no delay. In this case the attacker cannot be faster than the correct device. The attacker can be as fast as the correct device, but if two devices answer at the same time no correct data is received.

The second possible countermeasure is listening by the answering device to the channel during the time, it is open and the staring point of the transmission. The device could then detect an attacker, who wants to insert data.

The third option again is a secure channel between the two devices.

8.5 Man-in-the-Middle-Attack

As already outlined in previous section it is practically impossible to do a Man-in-the-Middle-Attack on an NFC link. The recommendation is to use active-passive communication mode such that the RF field is continuously generated by one of the valid parties. Additionally, the active party should listen to the RF field while sending data to be able to detect any disturbances caused by a potential attacker.

8.6 Secure Channel for NFC

Establishing a secure channel between two NFC devices is clearly the best approach to protect against eavesdropping and any kind of data modification attack.

Due to the inherent protection of NFC against Man-in-the-Middle-Attacks it is rather easy and straightforward to setup a secure channel.
A standard key agreement protocol like Diffie-Hellmann based on RSA or Elliptic Curves could be applied to establish a shared secret between two devices. Because Man-in-the-Middle is no threat, the standard, unauthenticated version of Diffie-Hellman works perfectly.

The shared secret can then be used to derive a symmetric key like 3DES or AES, which is then used for the secure channel providing confidentiality, integrity, and authenticity of the transmitted data. Various modes of operation for 3DES and AES could be used for such a secure channel and can be found in literature.

8.7 NFC Specific Key Agreement

Besides the standard key agreement mechanism, it is also possible to implement an NFC specific key agreement. This one does not require any asymmetric cryptography and therefore reduces the computational requirements significantly. Theoretically, it also provides perfect security. The scheme works with 100% ASK only and it is not part of the ISO standard on NFC. The idea is that both devices, say Device A and Device B, send random data at the same time. In a setup phase the two devices synchronize on the exact timing of the bits and also on the amplitudes and phases of the RF signal. This is possible as devices can send and receive at the same time. After that synchronization, A and B are able to send at exactly the same time with exactly the same amplitudes and phases.

While sending random bits of 0 or 1, each device also listens to the RF field. When both devices send a zero, the sum signal is zero and an attacker, who is listening, would know that both devices sent a zero. This does not help. The same thing happens when both, A and B, send a one. The sum is the double RF signal and an attacker knows that both devices sent a one. It gets interesting once A sends a zero and B sends a one or vice versa. In this case both devices know what the other device has sent, because the devices know what they themselves have sent. However, an attacker only sees the sum RF signal and he cannot figure out which device sent the zero and which device sent the one. This idea is illustrated in Figure 2. The top graph shows the signals produced by A in red and by B in blue. A sends the four bits: 0, 0, 1, and 1. B sends the four bits: 0, 1, 0, and 1. the lower graph shows the sum signal as seen by an attacker. It shows that for the bit combinations (A sends 0, B sends 1) and (A sends 1, B sends 0) the result for the attacker is absolutely the same and the attacker cannot distinguish these two cases.

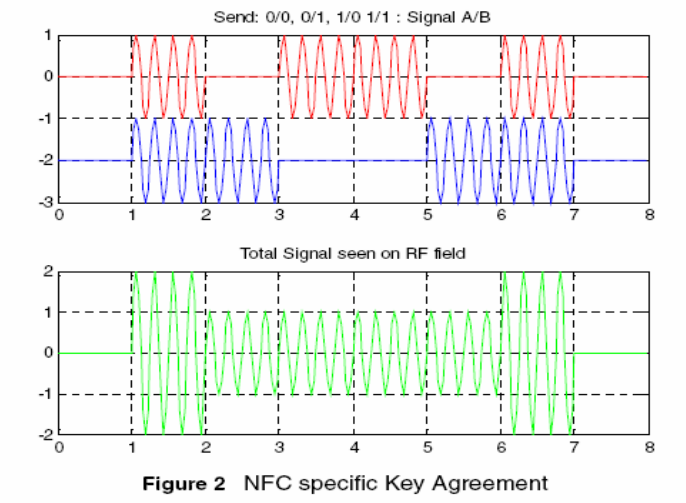


Figure 2 NFC specific Key Agreement

Source: Security in NFC, Reference No 2

The two devices now discard all bits, where both devices sent the same value and collect all bits, where the two devices sent different values. They can either collect the bits sent by A or by B. This must be agreed on start-up, but it doesn't matter. This way A and B can agree on an arbitrary long shared secret. A new bit is generated with a probability of 50%. Thus, the generation of a 128 bit shared secret would need approximately 256 bits to be transferred. At a baud rate of 106 Kbits/s this takes about 2.4 ms, and is therefore fast enough for all applications. The security of this protocol in practice depends on the quality of the synchronization which is achieved between the two devices. Obviously, if an eavesdropper can distinguish data sent by A from data sent by B, the protocol is broken. The data must match in amplitude and in phase. Once the differences between A and B are significantly below the noise level received by the eavesdropper the protocol is secure. The level of security therefore also depends on the signal quality at the receiver. The signal quality however again depends on many parameters (e.g. distance) of the eavesdropper. In practice the two devices A and B must aim at perfect synchronization. This can only be achieved if at least one of A or B is an active device to perform this synchronization.

Note, that in a recently published paper, the same idea for key agreement between an RF reader and an RF tag is presented in a slightly different setup. The paper uses a special so-called noisy tag. This noisy tag is a standard RFID tag, which acts as a third party inserting random looking bits into the communication from the real tag to the real reader. The reader however can calculate the bits sent by the noisy tag and can then calculate the bits sent by the real tag. The problem we see with this approach is that the noisy tag will not be able to do any synchronization with the real tag. This would be too complicated for a simple tag. Therefore, we think that this approach cannot work in practice. It would require a more sophisticated noisy device instead of the noisy tag to run that protocol in a secure way.

9. NFC-enabled handsets:

List of some NFC enabled handsets are:

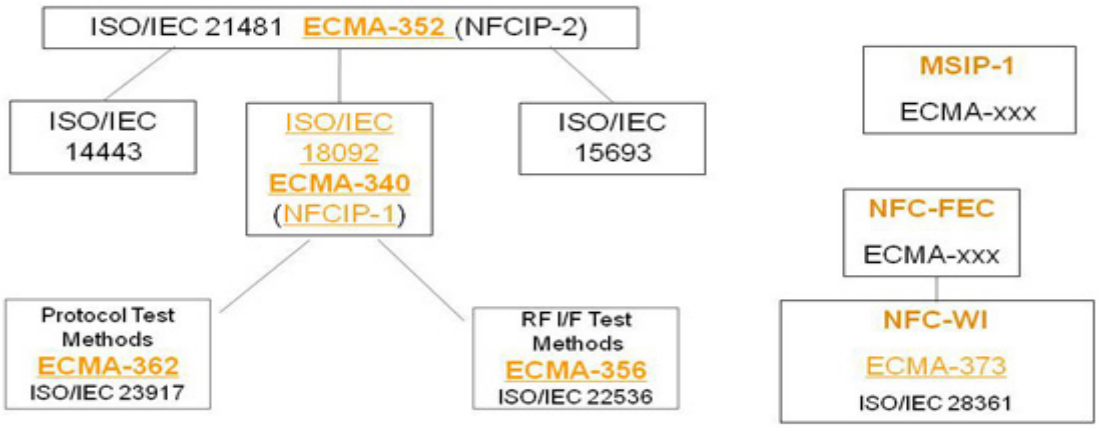
- Nokia C7
- Nokia 6216 Classic (Nokia has confirmed the cancellation of this phone in February 2010)
- Nokia 6212 Classic
- Nokia 6131 NFC

- Nokia 3220 + NFC Shell
- Samsung S5230 Tocco Lite/Star/Player One/Avila
- Samsung SGH-X700 NFC
- Samsung D500E
- SAGEM my700X Contactless
- LG 600V contactless
- Motorola L7 (SLVR)
- Benq T80
- Sagem Cosyphone
- Google Nexus S
- Etc.

10. Near Field Communication Interface and Protocol (NFCIP-1)

This Standard defines communication modes for the Near Field Communication Interface and Protocol (NFCIP-1) using inductive coupled devices operating at the centre frequency of 13.56 MHz for interconnection of computer peripherals. It also defines both the Active and the Passive communication modes of Near Field Communication Interface and Protocol (NFCIP-1) to realize a communication network using Near Field Communication devices for networked products and also for consumer equipment. This Standard specifies, in particular, modulation schemes, coding, transfer speeds, and frame format of the RF interface, as well as initialization schemes and conditions required for data collision control during initialization. Furthermore, this Standard defines a transport protocol including protocol activation and data exchange methods. Information interchange between systems also requires, at a minimum, agreement between the interchange parties upon the interchange codes and the data structure.
This 2nd edition fully matches ISO/IEC 18092.

ECMA-356 "NFCIP-1 - RF Interface Test Methods", and ECMA-362 "NFCIP-1 - Protocol Test Methods" specify tests for ECMA-340.
ECMA-373 specifies the two-wire interface between a Transceiver and a Front-end.



NFC protocol arrangement

Source: NFC protocol Arrangement, Reference No 4

11. Current trials

This section will give the broad view of international scenario (trials) of NFCs and its applications.

11.1 Europe

Austria

- Mobilkom Austria, University of Applied Sciences of Upper Austria, Samsung, NXP

Belgium

- NXP, Alcatel-Lucent touchatag, BUZY.BE, Belgacom Pingping

Bulgaria

- SEP Bulgaria

France

- Orange, Groupe LaSer and Vinci Park, Samsung, NXP in Caen
- Bouygues Telecom, RATP, Gemalto, NEC, Inside Contactless in the Paris Métro
- NRJ Mobile (MVNO), Crédit Mutuel, CIC, Master Card, Gemalto, Sagem, Inside Contactless in Strasbourg
- SFR, Crédit Mutuel, CIC, Master Card, Gemalto, Sagem, Inside Contactless in Strasbourg
- Bouygues Télécom, SEMITAG, Transdev, Gemalto, Sagem, Inside Contactless in Grenoble
- Orange, Veolia, Clear Channel, Laser Cofinoga in Bordeaux
- Bouygues Telecom, RATP, Cassis International, Sagem Orga in the Paris Métro
- Pegasus AEPM: multi-operator (Orange, Bouygues Telecom, SFR), multi-bank (BNP Paribas, Groupe Crédit Mutuel-CIC, Crédit Agricole, Société Générale) with MasterCard, Visa Europe, Gemalto and Oberthur Technologies for mobile payment in two cities: Caenand Strasbourg
- Nice, Ville NFC: AFSCM (Orange, Bouygues Telecom, SFR, NRJ Mobile), Gemalto, Oberthur Technologies, multi-bank (BNP Paribas, Groupe Crédit Mutuel-CIC, Crédit Agricole, Société Générale) with MasterCard, Visa Europe, Airtag, Toro, ConnectThings, Veolia Transport, Adelya and more (to be completed)

Finland

- City of Oulu, VTT
- Elisa, Gemalto,
- Red Solution Finland Oy

Germany

- Rhein-Main Verkehrsverbund (public transport authority), Vodafone, Nokia, NXP, Philips,
- Touch&Travel: Telekom Deutschland, Vodafone, Deutsche Bahn, Motorola, Giesecke&Devrient, ATRON electronic, Germany

Hungary

- InfomatiX Ltd. / MobiAccess development framework
- AFF Entry System, AFF Group
- NGMS Hungary EntryPoint, TiMOTHY]

The Netherlands

- Payter, nationwide roll-out of mobile payment wallet over-the-air
- Nedap NV Healthcare
- JCB, KPN, CCV Holland B.V., Gemalto, Nokia, PaySquare, NXP Semiconductors, Vivotech.
- Roda Stadium, KPN, Philips, Bell ID, SmartPoint
- Rabobank, Rabo Mobiel (MVNO), KPN, NXP, Albert Heijn

Norway

- Telenor and Cominor (public transport operator), NFC ticketing trial - using JavaCard emulation of MIFARE DESFire.

Poland

- Polkomtel, mPay — mobile payments

Romania

- ING ING Group, Toro, Collis: mobile payment solution

Sweden

- TeliaSonera and Västtrafik (public transport authority) testing ticket and traffic information via NFC.

Turkey

- BKM Bankalararasi Kart Merkezi (Turkey's national card switch and clearing centre BKM) multi-bank an multi-operator trial, with aCassis International TSM technology

United Kingdom

- Cheshire County Council, StaffPlan Connect time recording and point of care system
- Over-C, Welbeing Domicilary Care.
- Manchester City Football Club, Orange, Barclays, TfL Oyster card
- O2, Consult Hyperion at the Wireless Festival in Hyde Park (Wristband format)
- Transport for London, smart poster
- Barclays debit cards issued post March 2009

11.2 North America

Canada

- MasterCard, Bell Mobility, Vivotech, Société de Transport de Montreal

USA

- Mobile Transit Trial: Sprint, First Data, Bay Area Rapid Transit, Jack In The Box, Vivotech Western Union Speedpay
- Cingular Wireless, Citigroup, New York subway, MasterCard Worldwide, Nokia, Venyon
- ZTar (MVNO), Discover Financial Services, Motorola, NXP, Inside Contactless that can be used with phones, cards, key fobs, and other devices.
- 7-Eleven, Master Card in Dallas
- Nokia, Philips, Vivotech FlyBy at the Philips Arena in Atlanta
- Bank of America and Visa test for in-store payments in New York.

11.3 Asia and Oceania

Australia
- First Australian NFC mobile phone payment pilot, Commonwealth Bank of Australia, MasterCard, Vivotech
- Telstra, National Australia Bank, Cassis International on a Sagem Orga SIM card
- Queensland's TransLink Go card Service. Perth's TransPerth Transport Services.

China
- China Mobile, Philips, Nokia and Xiamen e-Tong Card

India
- Delta Technologies
- Citi Tap and Pay - Citibank India

Japan
- JCB Japan Credit Bureau, Cassis International experiment of OTA Services for NFC Mobile Payment

South Korea
- KTF and GSMA
- SKTelecom, Philips, Cassis International

Malaysia
- Visa, Maybank, Maxis, Touch'n'Go, Nokia, Cassis International (TSM services), Vivotech

Taiwan
- Taiwan Mobile, MasterCard, Taipei Fubon Bank and Vivotech
- Chunghwa Telecom, EasyCard, BenQ, NXP
- Chinese Culture University, Mos Burger
- Toro

Singapore
- Ez-link, Samsung, Cassis International
- Singtel, NETS, Vivotech

Thailand
- Thai E-purse Order (for seven-eleven markets and loyalty programs), Giesecke & Devrient, Germany; Thai Smart Card Group (TSC)
- KasikornBank, Gemalto, Toro, Visa

11.4 Latin America

Argentina
- RedBus Córdoba, Argentina.

Guatemala
- First NFC mobile payment pilot in Latin America Visa, VisaNet, Vivotech

11.5 Middle East

UAE
- First NFC mobile payment pilot in the Middle East and North Africa Emirates Integrated Telecommunications Co. PJSC – DU

12. Recommendations:

The following are recommendations for use of NFC applications in Pakistan.

- This consultation document should be placed on PTA website for comments of operators, vendors, users and all stakeholders.
- Implementation mechanism of NFCs should be discussed with all stakeholders (Telecom operators, vendors and Suppliers, Telecommunication Technology users, Ministry of IT, Frequency allocation board etc) at subsequent meetings at PTA with all concerned.
- On completion of the process of consultation a way forward to be chocked out by PTA for beginning NFCs in regulatory ambit and lawful applications.

References

1. http://en.wikipedia.org/wiki/Near_Field_Communication
2. http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf
3. http://www.check-in.aero/2010/08/nfc-enabled-mobile-phones-the-future-of-the-check-in-process/#
4. http://docbox.etsi.org/Workshop/2009/200901_SECURITYWORKSHOP/NXP_MEINDL_NFCIP1SecurityStandardProtectsNearFieldCommunication.pdf
5. http://www.differencebetween.net/technology/difference-between-rfid-and-nfc/
6. http://www.3gtech.info/tag/nfc-vs-bluetooth
7. http://www.gsmworld.com/documents/aa9310.pdf
8. http://www.gsmworld.com/documents/gsma_nfc2_wp.pdf
9. http://www.gsmworld.com/documents/faq_nfc_tech_vs2.pdf
10. http://www.gsmworld.com/documents/gsma_nfc_tech_guide_vs1.pdf
11. http://www.gsmworld.com/documents/GSMA_Requirements_For_SWP_NFC_Handsets_V2.pdf
12. http://www.itu.int/net/search/searchframe.aspx
13. http://www.ecma-international.org/publications/standards/Ecma-352.htm
14. http://www.radio-electronics.com/info/wireless/nfc/near-field-communications-tags-types.php
15. http://www.ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4299324
16. http://www.ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4454171
17. http://www.ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4351439
18. http://www.courses.engr.illinois.edu/ece445/projects/.../project31_presentation.ppt
19. http://nds1.nokia.com/phones/files/guides/Nokia_6131_NFC_UG_en.pdf
20. http://www.nfc-reader.com/acr122.php
21. http://www.springcard.com/blog/2010/nfc-tags-with-nfctool-and-nfcdecoder/
22. http://www.tiresias.org/research/guidelines/nfc.htm
23. http://www.eetimes.com/design/communications-design/4012606/How-NFC-can-to-speed-Bluetooth-transactions-151-today
24. http://www.nearfield.org/2007/03/bluetooth-21-incorporating-nfc