Inside NFC: Usages and Working Principles

This article explains NFC: how it works, what it can be used for and why its growing popularity and ease of use can add great value to applications.

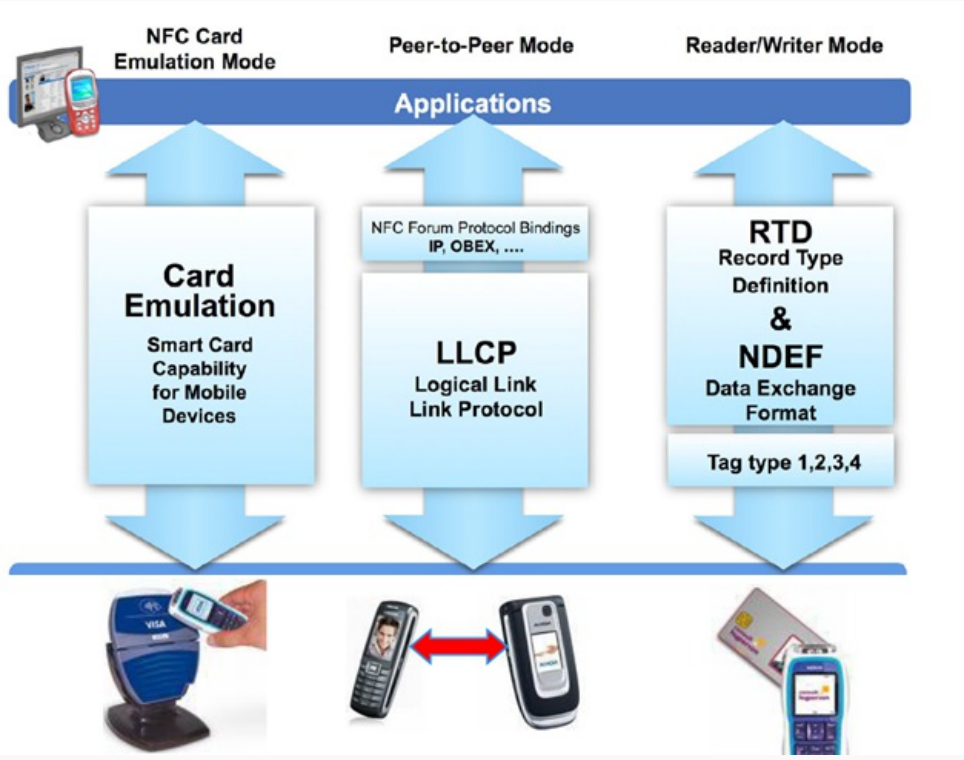
03 Jul 2011

Introduction

Near Field Communication (NFC) is a short range wireless connectivity technology standard. It is designed for simple and intuitive communication between all types of consumer devices. NFC works based on radio frequency identification (RFID) technology. This makes use of interacting electromagnetic radio fields instead of the typical direct radio transmissions used by technologies such as Bluetooth. It is meant for applications where a physical touch, or close to it, is required in order to maintain security. NFC can do much useful work with mobile phones, among other things, payment, in conjunction with an electronic wallet, and for setting up connections between Bluetooth devices etc.

Usages of NFC devices

NFC can be used in various ways and it is growing continuously. Following figure shows how many ways we can use NFC technology for different purposes. There are basically three main catagories.



Card Emulation mode

In this mode, NFC enabled phones appears to an external reader much the same as a traditional contactless smart card. For example, some confidential data such as Visa card number is written in the secure element of the phone and that data is read by the external reader and send the information for further processing. This enables contactless payments and ticketing by NFC enabled phones without changing the existing infrastructure. Mobile payment, ticketing access control etc are use case of this category.

Peer to Peer mode

In this mode two NFC enabled devices can exchange data with each other. Both devices take part in the communication. One example could be business card exchange. When we touch two devices with each other both devices can exchange business card. Another example could be pairing Bluetooth headset with the help of NFC enabled phone. Third example could be NFC chat application where two phones can take part in data exchange as specified by NFC forum.

Reader/Writer mode

In this use case, NFC enabled device (for example mobile phones) can read or write data to NFC tag (see later section of this document). NFC enabled smart poster is one example. Inside the poster there is embedded NFC tag where more information is

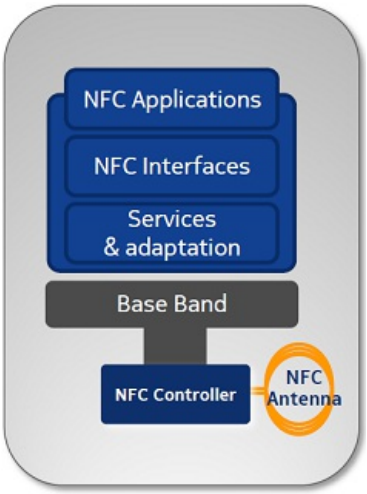
(C) Copyright Nokia 2014. All rights reserved.

written about the product. Device and read and act accordingly what is written in the tag. Another use case is electronic product code.

Many experts believe the 96bit electronic product code (EPC), as shown in the following figure, will be the next generation of the universal product code (UPC), the familiar general trade identification number imprinted in the barcode on a majority of products sold today.

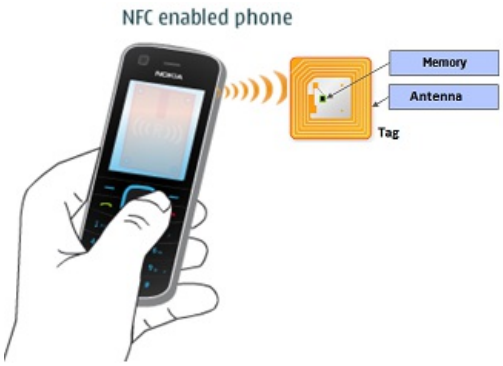
How Does NFC work

A radio frequency (RF) sine wave generated by the reader (phone) is used to transmit energy to the tag and retrieve data from the tag. When the NFC in the device is active then it continuously generates periodic sine wave signal at frequency 13.56 MHz center frequency. If there is any tag within the area of magnetic flux generated by the sinewave, tag gets energy from the magnetic fluxes and create counter frequency or change the frequency properties of the original sine wave generated by phone. The changes are detected by the phone and phone knows that there is a tag nearby. RFID systems communicating on very short range are commonly known as close couple systems. The range where communication is considered to be close coupled is between 0 and 1 cm. This means that the tag has to be placed either in the reader or more or less pressed against the reader device. The benefit from these short distances is that a rather large amount of energy can be extracted from the magnetic field by the tag. More energy is available for signal processing in the tag at this distance without the need for a power supply in the tag. Close coupling is also preferred for systems with high security requirements. Following figure shows some simplified relation between NFC application to NFC hardware.



Reader

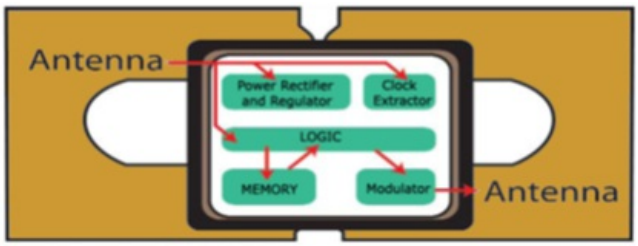
Usually a microcontroller-based (for example NFC enabled phones) with an integrated circuits that is capable of generating radio frequency at 13.56 MHz with other components such as encoders, decoders, antenna, comparators, and firmware designed to transmit energy to a tag and read information back from it by detecting the backscatter modulation. The reader continuously emits RF carrier signals, and keeps observing the received RF signals for data. Following figure shows how phone generates RF signal and how tag antenna get power from it.



(C) Copyright Nokia 2014. All rights reserved.

Tag

An RFID device incorporating a silicon memory chip connecting to external antenna. Tag does not have its own power source. The passive tag absorbs a small portion of the energy emitted by the reader (phone), and starts sending modulated information when sufficient energy is acquired from the RF field generated by the reader. Note that the data modulation (modulation for 0s and 1s) is accomplished by either direct modulation or FSK or Phase modulation. Following figure shows the internal hardware of NFC tag where we can see its memory, logic etc.

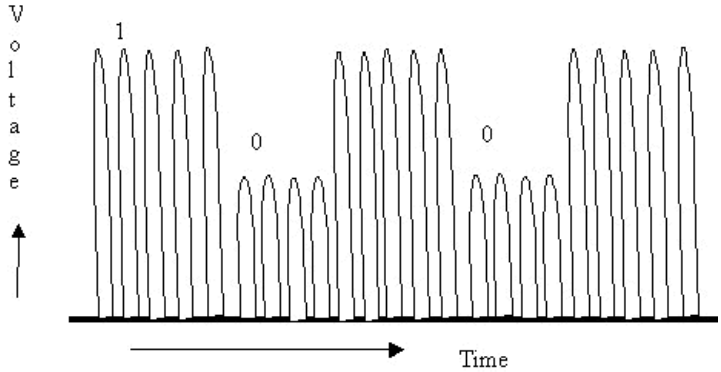


The most common of these is a “passive” tag (shown above), so-called because it has no internal battery power. Instead, passive tags are powered by energy drawn from the RF carrier wave transmitted by the reader. Following are the types of tag-

1. NDEF tag-NFC data exchange format
2. Mifare 1k tag

Modulation and Data transfer

Modulation is the process of modifying the characteristics of a signal, called a carrier wave, to convey information. The carrier wave for NFC is 13.56 MHz. The characteristics of a signal to modify include amplitude, frequency, and phase. Data are communicated on an RF carrier wave via a process called modulation. In this process a stream of data pulses (″1″s and ″0″s) are added to (mixed with) the carrier wave. The data stream has a clock frequency that is much slower than the carrier wave frequency. When data is added to the carrier frequency then the properties (amplitude and/or frequency and/or phase) are changed. The changes are detected by phones and it decodes the data send to upper level for further processing.
The carrier wave induces a small alternating current (AC) in the antenna. Inside the integrated circuit chip a power rectifier and regulator converts the AC to stable DC and uses it to power the chip, which immediately “wakes up”. The Clock Extractor separates the clock pulses from the carrier wave and uses the pulses to synchronize the logic, memory, and modulator sections of the tag’s IC chip with the reader. The logic section separates the 1’s and 0’s from the carrier wave and compares the data stream with its internal program to determine what response, if any, is required. If the logic section decides that the data stream is valid, it accesses the memory section for the chip’s unique identification data and any user data that have been stored there. The logic section encodes those data using the clock extractor pulses. The encoded data stream is input into the modulator section. The modulator mixes the data stream with the carrier wave by electronically adjusting the reflectivity of the antenna at the data stream rate. Electronically adjusting the antenna characteristics to reflect RF is referred to as backscatter. Backscatter is one of the most widely used modulation schemes for modulating data on to RF carrier. In this method of modulation, the tag coil (load) is shunted depending on the bit sequence received. This in turn modulates the RF carrier amplitude as shown in the diagram below. The reader detects the changes in the modulated carrier and recovers the data. Following figure shows how data is modulated with simplified amplitude modulatation to carry binary data.



The above diagram provides a simplified modulated carrier signals from the RFID tag. As seen in the diagram, the encoded binary digits modulate RF carrier. A 1 is represented with high carrier level, and a 0 is represented by a low carrier level (tag coil shunted). The reader demodulates the signals to recover the data, and note that this data is still encoded. The reader decodes the data using suitable decoder, and forwards it for further processing to a with NFC stack that runs in our phone. And finally it comes

(C) Copyright Nokia 2014. All rights reserved.

to our application.

Summary of data transfer

1. The reader continuously generates an RF carrier sine wave, watching always for modulation to occur. Detected modulation of the field would indicate the presence of a tag.
2. A tag enters the RF field generated by the reader. Once the tag has received sufficient energy to operate correctly, it divides down the carrier and begins clocking its data to an output transistor, which is normally connected across the coil inputs.
3. The tag's output transistor shunts the coil, sequentially corresponding to the data which is being clocked out of the memory array.
4. Shunting the coil causes a momentary fluctuation (dampening) of the carrier wave, which is seen as a slight change in amplitude of the carrier.
5. The reader peak-detects the amplitude modulated data and processes the resulting bit stream according to the encoding and data modulation methods used.

References

1. http://www.eetimes.com/design/microwave-rf-design/4018928/Radio-Basics-for-RFID-Modulation-and-Multiplexing/
2. http://www.rfid-handbook.de/rfid/types_of_rfid.html
3. http://www.tutorialsweb.com/rfid/operation-of-rfid-systems.htm
4. NFC_Forum_Mobile_NFC_Ecosystem_White_Paper.pdf
5. Basic Concepts of RFID.pdf
6. EEOL_2009JUL17_RFD_DT_TA_01.pdf
7. http://www.developer.nokia.com/info/sw.nokia.com/id/bdaa4a0f-fcf3-4a4b-b800-c664387d6894/Introduction_to_NFC.html

(C) Copyright Nokia 2014. All rights reserved.