

NFC

Technical Overview

Release r04

Trademarks

The Bluetooth® word mark and logos are owned by the Bluetooth SIG, Inc. and any use of such marks by Stollmann E+V GmbH is under license. Other trademarks and trade names are those of their respective owners.

Copyright © 2005-2008 Stollmann E+V GmbH

Table of contents

1	Abstract	5
2	NFC	5
3	Definitions	5
3.1	Tag	5
3.2	ContactlessCard	6
3.3	Reader/Writer	6
3.4	RFID	6
3.5	ContactlessCard transmission.....	6
3.6	Secure element.....	7
4	Applications	7
4.1	Identification / Authorization	7
4.2	Transmission of information	8
4.3	SmartPoster.....	8
4.4	MobilePayment.....	8
4.5	MobileTicketing.....	8
4.6	Transportation.....	8
4.7	SimplePairing.....	9
4.8	Access Control.....	9
5	Technology	9
5.1	RF transmission.....	9
5.2	Energy transmission	9
5.3	CardEmulation	10
5.4	Reader/Writer	10
5.5	Peer-to-peer.....	10
5.6	ModeSwitch	11
5.7	NDEF	11
6	Integration.....	12
6.1	Chips	12

6.2	Modules	12
6.3	JSR-257	12
6.4	PC-SC	13
6.5	Proprietary APIs.....	13
6.6	Command Interface	13
6.7	Toolkits	13
7	Application development.....	13
7.1	Mobile phone	13
7.2	PC	14
7.3	Embedded systems	14
8	History	14

1 Abstract

Short-range radio technology Near Field Communication (NFC) is based on RFID and promises to support new usage models for mobile applications. By taking a “touch and ...“ approach it simplifies the selection, configuration and adaptation of wireless devices and connections in many applications. Currently integrated into mobile phones NFC will also be found in embedded devices for the communication with phones, PCs, contactless cards and RFID tags and readers. The presentation outlines the technical features of NFC and the main usage models and gives hints for the integration of NFC in embedded devices.

2 NFC

Near Field Technology (NFC) is a wireless transmission technology that can transmit data at high speeds of up to 424 kbps over very short distances of up to 10 cm. NFC is based on ContactlessCard and RFID technology and is to a large extent compatible with them. However, while ContactlessCards and RFID practically always require an asymmetrical transmission with an active reader/writer and a passive tag or a passive card, NFC expands it by a symmetrical, □bi-directional transmission between devices with balanced links – the peer-to-peer mode.

For this reason, sharp distinctions between NFC, RFID and ContactlessCard technology are frequently not made. In particular, the integration of mobile phones and PDAs always refers to NFC, even if the peer-to-peer mode is not (yet) being used in many applications, but the RFID or ContactlessCard basic technologies. This is important when it comes to evaluating the specification and implementation status of certain standards and to what extent they can currently be used in mass-manufactured products.

3 Definitions

First, we will define a few terms that are important in the discussions surrounding NFC applications and devices.

3.1 Tag

A tag is a non-volatile data carrier that can be read and possibly written using radio technology. Most tags are passive, i.e. they do not have their own power supply but, instead, are powered by the electromagnetic field of the reader/writer. During the reading, the tag modulates the field and transmits the data. The amount of information that can be stored in tags varies greatly and typically measures in the range of some ten bytes and several tenkilobytes. The larger the memory, the longer the reading takes, which is problematic in many applications and, therefore,

reduces the practical usable memory size. Some tags feature a fixed content that cannot be changed. Others can also be written with new information.

3.2 ContactlessCard

A ContactlessCard is a contact-free chip card that can be read via NFC. It features the same properties as a tag. In addition, it frequently features a secure element that contains sensitive information in encrypted form.

3.3 Reader/Writer

A reader/writer is a device that can read tags and ContactlessCards and write to them. To be able to communicate with passive tags and ContactlessCards, it establishes an electromagnetic field from which the tag or ContactlessCard draws its operating energy and which is modulated for data transmission. Reader/writer can be designed in such a way that they can read from and write to RFID tags as well as ContactlessCards of different types.

3.4 RFID

RF identification (RFID) refers to a series of specifications that describes the identification via radio technology. RFID is used particularly as a replacement of barcodes and operates in different frequency ranges (several kHz to GHz) with different transmission ranges (cm to several meters) and with passive (without own power supply) and active (with own power supply) tags. Of these RFID specifications, NFC uses only the frequency of 13.56 MHz with passive tags.

3.5 ContactlessCard transmission

There are several standards for contactless transmission. The best known is ISO 14443, which differentiates between Type A and Type B. The ISO 14443 Type A contactless card was originally intended to be a memory card only. However, microprocessor and cryptographic cards have been developed for Type A. The most common Type A cards are the Mifare cards which is a contactless Smart Card technology owned by NXP. Mifare is an open architecture platform and has more than 300 million cards in the field worldwide. The ISO 14443 Type B contactless card was originally intended to be microprocessor version of Type A. Again, the memory and cryptographic options have been added for Type B. The Type B cards are not as commonly deployed as Type A cards. Calypso, an international standard for electronic ticketing is ISO 14443 Type B compliant as well as contactless payment standards MasterCard PayPass and VISA Wave.

Another well known Standard is Felica. FeliCa is a contactless RFID IC chip smart card system by Sony, primarily used in electronic money cards. Which is widely spread in the far east. Especially in Japan.

3.6 Secure element

A secure element (SE) contains an embedded processing element which ensures that the outside communication is processed in encrypted form and stores protected information that should only be made accessible only under certain conditions. The protected data is transmitted in encrypted form using an NFC interface. From the point of view of NFC, it represents application data for the NFC interface that are transmitted without being changed. From that point of view, NFC and secure element are independent of each other. However, since many NFC systems (mobile phones, ContactlessCards, etc.) also feature a secure element, the communication between NFC interface and secure element plays an important role in system integration.

4 Applications

NFC follows two important objectives. On the one hand, a standard is being introduced to the mass market; on the other hand, this standard is backward compatible with existing solutions.

NFC enables a series of applications, whereby the compatibility with RFID or ContactlessCards is an important condition for some of them. The paradigm of all NFC applications is that the user holds a device – typically a mobile phone or PDA – to a certain point – a tag, ContactlessCard, reader or another NFC device – and triggers an action. This “touch-and-...” is a very simple way of triggering an action, much simpler than having to search in a menu for compatible devices, entering web links, or something similar. In addition, storing event tickets in a mobile phone, for example, facilitates applications by doing away with issuing paper tickets and providing a stronger integration of process flows.

4.1 Identification / Authorization

The user holds the NFC device against a reader and is then being identified and authorized. This can be used for mobile payments, access control, entrance to events, etc. To secure certain authorizations (such as payments), the entry of a PIN may also be required.

4.2 Transmission of information

The user holds the NFC device against a tag or another NFC device and receives data. This can be product information, business cards, or information for access to LANs or Bluetooth devices.

4.3 SmartPoster

In this application case, an RFID tag is positioned on a poster. It contains data that are coded according to the NDEF specification. This allows them to be read by any NFC device (e.g. a mobile phone). The tag may contain additional product information or a link to a website that contains additional information.

4.4 MobilePayment

In this application case, the NFC device (e.g. the mobile phone) replaces the credit card. The credit card information is stored on the mobile phone in a secure element. The user holds the mobile phone against the credit card reader, which reads the credit card information from the secure element of the mobile phone. For larger amounts, the entry of a PIN is required. To read the secure element, most concepts rely on a JAVA application on the mobile phone which is issued by the credit card company.

4.5 MobileTicketing

A ticket is stored on the NFC device (e.g. a mobile phone) after, for example, an NFC-based payment transaction. At the place of the event, the user holds the mobile phone against the ticket reader and obtains access to the event. For this purpose, the mobile phone behaves like a tag. In addition, information about the event can be transferred to the mobile phone.

4.6 Transportation

Different concepts are used here. In one concept, the NFC device (e.g. a mobile phone) is held against a tag at a transit stop. It reads the information and uses it to generate a ticket. Upon departing at the destination, the passenger holds it against a tag again at the transit stop. Based on this information, the mobile phone calculates the overall distance.

In another scenario, the reader in the 'means of transportation' (e.g. bus, railroad) transfers the identification of the mobile phone to a server that generates and bills the ticket.

In addition to the transit stop information, other data can be exchanged that require the peer-to-peer mode.

4.7 SimplePairing

Until now, it is complicated to establish the connection between two Bluetooth devices (pairing). This requires searching for other devices, analyzing the profiles and subsequently pairing them. This process can be greatly facilitated by using NFC. By holding the NFC devices against each other, they exchange the pairing information for Bluetooth and afterwards, they can immediately establish the connection. It can be used for different Bluetooth profiles (data exchange, voice transmission). Furthermore, the pairing information can also be used in other contexts. For example, the mobile phone can briefly be held against the handsfree communication device when entering the car to indicate who the driver is who wants to use the hand-free communication device to avoid assignment conflicts with mobile phones of passengers.

4.8 Access Control

Access control data to a building are stored on the NFC device (e.g. a mobile phone). Upon entering the building, the mobile phone is read by the reader. Furthermore, additional information, such as dates, can be transferred to the mobile phone via the peer-to-peer mode.

5 Technology

5.1 RF transmission

The RF transmission of NFC uses the 13.56-MHz frequency that is also used for certain RFID types and ContactlessCards. Hence, NFC is compatible with these transmission procedures.

The sender that builds up the field is the reader/writer. It constantly transmits using the frequency of 13.56 MHz. The tag modulates the field by means of load modulation. The reader/writer measures the load of the field and extracts the data from the modulation.

The modulation of the field for all compatible technologies combined under NFC is identical.

5.2 Energy transmission

Passive tags without their own power supply can draw the energy required for reading the memory, operating the own processor and memory systems, and modulating the field from the field itself. This requires a sufficiently large magnetic flux that must be built up by the reader/writer. In turn, this requires antennas with a sufficient dimension. The decisive factor is the area enclosed by the antenna. For

this reason, it is often advantageous to integrate the antenna in the housing and route it in windings at the edge of the housing.

The power that tags can draw from the field measures in the order of magnitude of a few mW. Furthermore, it is often available only for some milliseconds as long as the tag is held in front of the reader/writer. Hence, it is sufficient only for very simple operations, such as reading a moderately sized memory of several kilobytes. More complex tasks that require a higher CPU power cannot be handled with it.

The program of a tag must also be robust so that it is not damaged by accidental loss of the power supply.

Active devices with their own power supply do not draw energy from the field of the reader/writer. For this reason, NFC devices that are intended to communicate exclusively with active devices can be equipped with smaller antennas.

5.3 CardEmulation

ContactlessCards based on the specifications of Mifare, Felica and ISO 14443B, can be read by NFC devices. If NFC devices need to be read by card readers, they must themselves behave like a ContactlessCard. This application is specified by the CardEmulation.

The CardEmulation encompasses the RF behavior and the way how a ContactlessCard is read. The formats in which the data are stored on ContactlessCards are partially application-specific. The NFC forum standardized several formats, but NFC devices must also support other formats in the near future if they want to be compatible with the existing ContactlessCards.

The CardEmulation also includes the emulation of tags. In principle, it works exactly like the CardEmulation, only that the RFID tags, in turn, have their own transmission and data formats with which NFC devices must be compatible so that they can be read.

5.4 Reader/Writer

NFC devices can be read and possibly written as reader/writer tags or ContactlessCards. In this mode, they must also meet the existing specifications for ContactlessCards and tags. Similar to the CardEmulation, this also includes the formats in which the data are stored.

5.5 Peer-to-peer

The peer-to-peer mode is not supported by ContactlessCards and tags and is exclusively specified between true NFC devices. Both devices are active in this

mode, i.e. they have their own power supply and do not draw their operating energy from the RF field.

Protocols are specified for the peer-to-peer mode that are used for the data exchange between the devices. They allow a secure, □bi-directional transmission of data packets so that even larger data volumes, such as photos, files, etc., can be exchanged between NFC devices.

5.6 ModeSwitch

If an NFC device discovers another device in the radio field, it must first determine whether this is a ContactlessCard, an RFID tag, a reader/writer or another NFC device. This is accomplished by the ModeSwitch specification. It ensures that the NFC device goes to a status in which it can communicate with the other device in the radio field. It also defines the responses if several cards are found in the field at the same time and other potential error cases.

5.7 NDEF

NDEF stands for “NFC Data Exchange Format” and is a data format defined by the NFC forum for the exchange of information between two NFC forum devices or an NFC forum device and an NFC forum tag.

The NDEF specification provides clear rules for the structure of a corresponding message, without restricting the type of information it contains. This allows encapsulating the most diverse data, such as URLs, images or XML documents. However, the specification does not encompass any NDEF transmission protocol. Hence, the type of medium for the transmission of messages is also freely selectable, just like the type of information it contains. An NDEF message consists of a series of NDEF records. As a result, the actual encapsulation of the data takes place in the individual NDEF records.

Some widely used specific data formats, e.g. URI, Text, SmartPoster, are standardized by the NFC-Forum as Record Type Definitions (RTD) to allow interoperability of products of different vendors.

To allow an efficient analysis of the information contained in the records, the type and size of the data can be identified via the header. To enable a simpler identification, a number of different types of information have already been defined through the NFC forum. Beyond that, it is, however, possible to define any number of additional types.

6 Integration

6.1 Chips

The bases for integrating NFC in devices are NFC chips. They contain at least the radio technology with the RF modulation and the basic radio protocols. They often also contain an additional CPU that can process additional protocol layers.

The control of the hardware requires software that is specifically tailored to the chip. It is generally supplied by the chip manufacturer. It can subsequently be used by protocol stacks via an API.

With higher integrated chips, the hardware-dependent software is integrated directly on the chip. Even more processing power is provided by chips that can also carry the higher layers of the protocol stacks and the application software.

NFC can also be integrated in other chips. This is particularly interesting where larger systems, such as chips for mobile phones or Bluetooth chips, must be expanded by the NFC functionality.

6.2 Modules

Since the integration of NFC chips in a layout is not very simple, modules are frequently used that carry the NFC chip and additional components on a small circuit board. In particular, they contain the RF components. Furthermore, modules can contain additional functions, such as the higher layers of the protocol software, to free the device in which the module is integrated from these tasks. This also facilitates the software integration since the entire NFC technology can be encapsulated in the module and can then be controlled, for example, via a serial interface with AT commands.

6.3 JSR-257

To control an NFC interface in a device requires an API. If a JAVA environment is available, NFC can be used via the JSR-257 API. JSR-257 provides a series of functions that can be called by the application software to execute or initiate actions on the NFC interface.

However, JSR-257 supports only functions for the CardEmulation and reader/writer mode. The functions of the peer-to-peer mode cannot be controlled via JSR-257 yet. An expanded specification is expected for this purpose.

The JSR-166 API can be used in a JAVA environment for access to the secure element.

A JSR-257 can be integrated into the mobile phone by the developers of the mobile phone. It may also come with the JAVA VM if it has been integrated by the JAVA VM vendor.

6.4 PC-SC

If a secure element is connected with a PC, it is generally addressed via a PC-SC driver. It provides the PC-SC-API which is used by the application software as access interface to the secure element. The PC-SC communication may be routed transparently via NFC not affecting the content.

6.5 Proprietary APIs

Since no API has been standardized for the complete NFC protocol stack until now, the manufacturers defined their own APIs. For this reason, application programmers must adjust their programs to the corresponding APIs if they want to use a specific NFC protocol stack for the data transmission.

6.6 Command Interface

Serial modules, in which the complete NFC protocol stack is already integrated, have their own command interface. Card Emulation and reader/writer communication runs largely transaction-oriented and generally requires no additional intervention. The parameterization of the module typically differs from module manufacturer to module manufacturer.

6.7 Toolkits

To simplify the integration of NFC protocol stacks and modules, manufacturers developed toolkits that contain sample applications, source codes and evaluation platforms. These toolkits are the easiest way of gaining an overview of the NFC technology and selecting a manufacturer as partner for the NFC integration.

7 Application development

The development of NFC applications is heavily dependent on the platform used. Three essential platforms can be differentiated.

7.1 Mobile phone

An NFC interface generally uses a driver in a mobile phone that provides a JSR-257 API under JAVA. A JAVA application software on the mobile phone can use this

interface to access the NFC functions. The following is required to program the application software:

- Development kit for the JAVA virtual machine. It can generally be downloaded from the website of the VM manufacturer, e.g. from Sun.
- Development kit of the mobile phone manufacturer. It contains the specific parts of the JAVA environment for the corresponding mobile phone. It also contains the parts required for programming the JSR-257.

In the future, there may be additional interfaces on mobile phones that provide the NFC functions. The exact architectures, which will then be possible, are currently still under development.

7.2 PC

To be able to use NFC with a PC, an NFC-USB adapter is generally used. It contains the NFC chip and the antenna. A driver, which must be tailored specifically for the adapter, is installed on the PC. It can provide a manufacturer-specific API that can be used by the application software. For this purpose, it must be adapted to the API.

The driver for the NFC-USB adapter can also provide a virtual serial interface (VCOMM port) with which the data can be sent to the NFC-USB adapter. A specific command language can be used to control the adapter.

7.3 Embedded systems

Embedded systems generally feature special processors and operating systems. For this reason, NFC modules are frequently used that contain the entire NFC functionality and, therefore, are easy to integrate. The application development then encompasses the control of the interface of the NFC module and the integration of the functionality in the overall system.

An alternative consists of porting the NFC protocol stack to the embedded system. In that case, an NFC chip or NFC module with lesser functionality can be used, which reduces the unit costs, but generates a higher development effort. In this case, the application software must be adapted to the NFC protocol stack used since no standardized API is available at present.

8 History

Version	Release Date	By	Change description
r01d00	01.02.07	Fh	Draft
r01d01	08.10.07	Cl	Modifications

r01d02	21.11.07	Fh	First version
r01d03	21.11.07	Bg	New template
r01	04.12.07	fh	First release version
R02	09.01.08	Fh	Removed disclaimer Chapter 6.6 Command Interface updated
r03d01	09.01.08	Cl	Typos, RTD
r03d02	13.01.08	Km	Typos, language
R03d03	14.1.08	NK	Typo
r04	09.04.2008	fh	Revised Chapter 3.5

Stollmann Entwicklungs- und Vertriebs-GmbH
Mendelssohnstraße 15 D
22761 Hamburg
Germany

Phone: +49 (0)40 890 88-0
Fax: +49 (0)40 890 88-444
E-mail: info@stollmann.de
www.stollmann.de