Near Field Communication (NFC) Technology and Measurements

White Paper

Near Field Communication (NFC) is a new short-range, standards-based wireless connectivity technology, that uses magnetic field induction to enable communication between electronic devices in close proximity. Based on RFID technology, NFC provides a medium for the identification protocols that validate secure data transfer. NFC enables users to perform intuitive, safe, contactless transactions, access digital content and connect electronic devices simply by touching or bringing devices into close proximity.
This White Paper gives an overview of NFC uses, NFC technology and signals and RF measurements on NFC units.

ROHDE&SCHWARZ

White Paper

Roland Minihold - 06-2011
1MA182_5e

SES-2007
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table of Contents

1 Abstract 3

2 NFC Use Cases 4

3 Basics of Data Transmission with NFC 5

4 NFC Technology and Signals 8

4.1 NFC Standards Evolution 8

4.2 NFC Operating Modes, Modulation and Coding 10

4.3 NFC Tag Types 12

5 NFC RF Measurements 13

5.1 Test Setups 13

5.2 NFC Forum Reference Devices 14

5.3 RF Tests on NFC Devices 15

Abbreviations 16

6 Literature 17

1 Abstract

Near Field Communication (NFC) is a new, short-range wireless connectivity technology that evolved from a combination of existing contactless identification and interconnection technologies. It was jointly developed by Sony and NXP Semiconductors (formerly Philips).

NFC is designed to enable the exchange of various types of information, such as telephone numbers, pictures, MP3 files or digital authorizations between two NFC enabled devices like mobile phones, or between an NFC enabled mobile phone and a compatible RFID chip card or reader that are held close to each other. NFC is intended to be used as an access key to contents and for services such as cashless payment, ticketing and access control.

NFC operates in a frequency range centered on 13.56 MHz and offers a data transmission rate of up to 424 kbit/s within a distance of approximately 10 centimeters. In contrast to the conventional contactless technology in this frequency range (only active-passive communications), communications between NFC-capable devices can be active-active (peer-to-peer) as well as active-passive, NFC therefore represents a link to the RFID world. NFC is backwards compatible with the widely used Smart Card infrastructure based on ISO/IEC 14443 A (e. g. NXP's MIFARE technology) and ISO/IEC 14443 B as well as with the Sony FeliCa card (JIS X 6319-4). For the exchange of information between two NFC devices, a new protocol was developed which is defined in the standards ECMA-340 and ISO/IEC 18092. The NFC Forum was founded in the year 2004 by NXP, Sony and Nokia to harmonize the NFC technique and to stimulate its deployment. The NFC forum develops specifications which ensure interoperability of NFC units and services. All of the above mentioned standards (ISO/IEC 14443 A, B, ISO/IEC 18092 und JIS X 6319-4/FeliCa) are included. The NFC Forum certifies NFC units compatible to its specifications from December 2010 onwards.

To ensure interoperability between mobile phones and RFID chip cards of different manufacturers, digital protocol tests and RF measurements are required on NFC devices. The RF measurements essentially include timing measurements, the measurement of signal strength in polling mode, carrier frequency measurement, reception sensitivity in polling mode, and the measurement of load modulation (signal strength of the listener signal).

2 NFC Use Cases

Many possible NFC applications are being considered. The special advantage of NFC is its straightforward mode of use. Simply touch or place a device close to something to initiate the desired service. Some typical uses are:

- Mobile payment
  - Pay with NFC phones for tickets or taxi rides
  - Pay with NFC phones at contactless POS (point of sales)
  - Store vouchers on NFC phones

- Authentication, access control - store electronic keys, legitimations on NFC phones
  - Secure building access
  - Secure PC log-in
  - Unlock car doors
  - Setup your home office with a touch by your NFC phone

- Data transfer between different NFC-units (peer-to-peer data exchange) like NFC-smart phones, digital cameras, notebooks, etc.
  - Exchange electronic business cards
  - Print out photos by holding the camera close to printer

- ‘Unlock’ another service (such as opening another communication link for data transfer)
  - Setting up Bluetooth, WLAN links

- Access to digital information
  - Read schedules from smart poster to NFC phone
  - Download maps from smart poster to NFC phone
  - Record location such as a parking in NFC phone

- Ticketing
  - Store theater / attraction / event tickets on NFC phone

3 Basics of Data Transmission with NFC

Like the RFID Standards 14443 and FeliCa NFC uses an inductive coupling. Similar to the transformer principle, the magnetic near-field of two conductor coils is used to couple the polling device (initiator) and listening device (target).

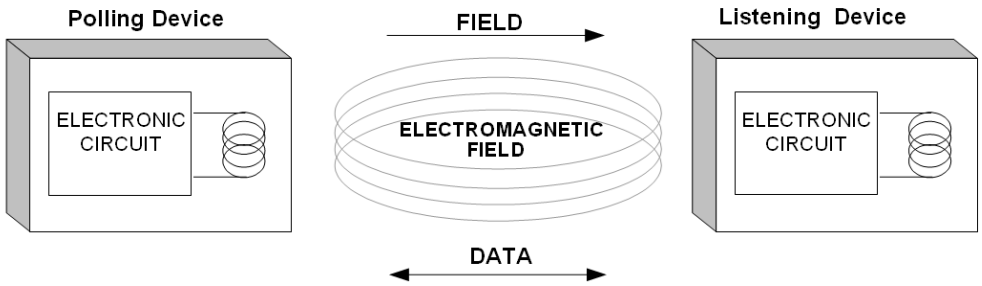

Figure 1: Polling device (initiator) and listening device (target) configuration [15]

The operating frequency is 13.56 MHz, and a bitrate of 106 kbit/s (partly also 212 kbit/s and 424 kbit/s) is used. Modulation schemes are amplitude on/off keying (OOK) with different modulation depth (100 % or 10 %) and BPSK.

Power Transmission and Data Transmission from a Polling Device

For transmission to a passive system such as an NFC phone in passive card emulation mode, the passive system uses the 13.56 MHz carrier signal of the polling device as energy source. Modulation scheme of the polling device is ASK.
For NFC peer-to-peer mode, both directions are modulated and coded like a polling device. However less power is necessary because both NFC devices use their own power supply and the carrier signal is switched off after end of transmission.

Data Transmission from a Listening Device

Due to the coupling of the coils of a polling and a listening device, a passive listening device also affects the active polling device. A variation in the impedance of the listening device causes amplitude or phase changes to the antenna voltage of the polling device, detected by the polling device. This technique is called load modulation. Load modulation is carried out in listening mode (as with ISO/IEC 14443) using an auxiliary carrier at 848 kHz which is modulated by the baseband and varies the impedance of the listening device. Figure 2 shows the spectrum with load modulation. The modulation scheme is ASK (as with ISO/IEC 14443 A PICC's) or BPSK as with 14443 B PICC's). There is a third passive mode which is compatible to FeliCa where the load modulation is without an auxiliary carrier directly as ASK on the 13.56 MHz carrier.

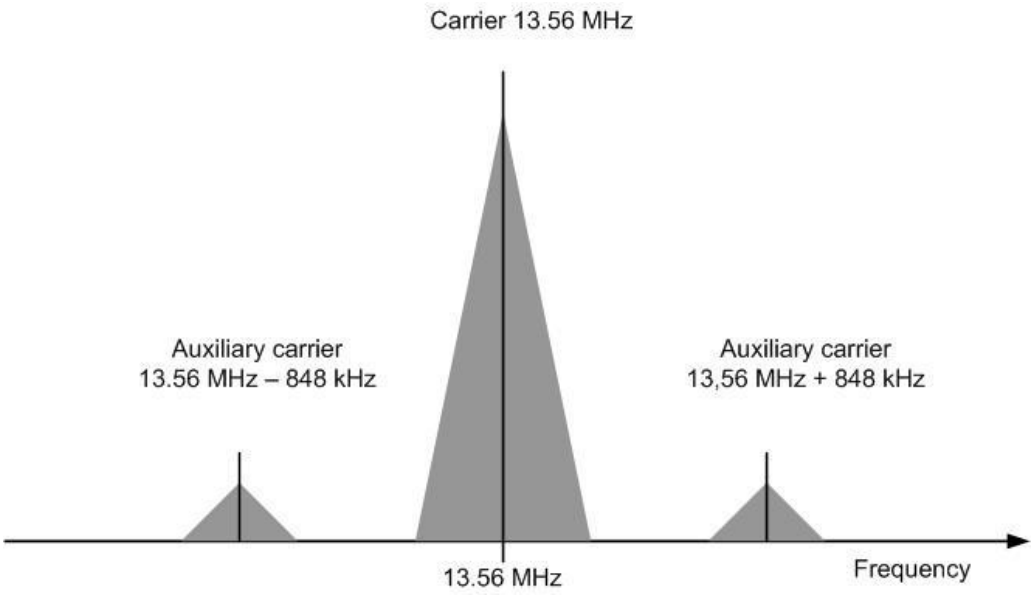

Figure 2: Load modulation on a 13.56 MHz carrier with 848 kHz auxiliary carrier. Modulation spectra of carrier and auxiliary carriers are indicated with triangles (Modulation spectra of carrier and of auxiliary carriers do not appear at the same time because NFC uses time division multiplexing).

Modulation Scheme and Coding

Amplitude shift keying (OOK) with different modulation depths (100% or 10%) or BPSK (as with ISO/IEC 14443 B PICC's) is used.

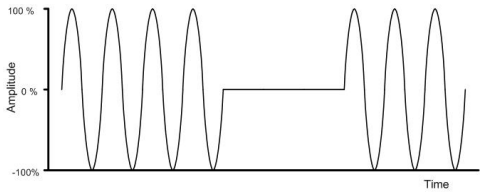

Figure 3:ASK with 100% modulation depth

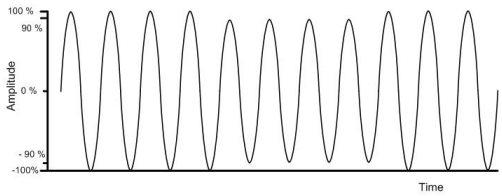

Figure 4: ASK with 10% modulation depth

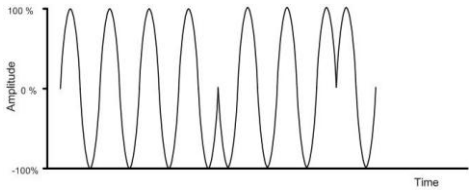

Figure 5: BPSK modulation

NRZ-L, Modified Miller and Manchester Coding are used by NFC.

- With NRZ-L a “high”-state during a bit duration indicates a logic 1, a “low”-state a logic 0.
- With Manchester Coding the first half of a bit will be set to “high”-state at a logic 1, and the second half to “low state”. With a logic 0, the fist half of a bit is set to “low”-state and the second half to “high”-state.
- With Modified Miller Coding with a logic 1 a “low” pulse occurs after half of the bit duration. With a logic 0 a “low”-pulse occurs at the beginning of a bit. Exception: If a logic 0 follows a 1 no pulse occurs, the signal remains high.

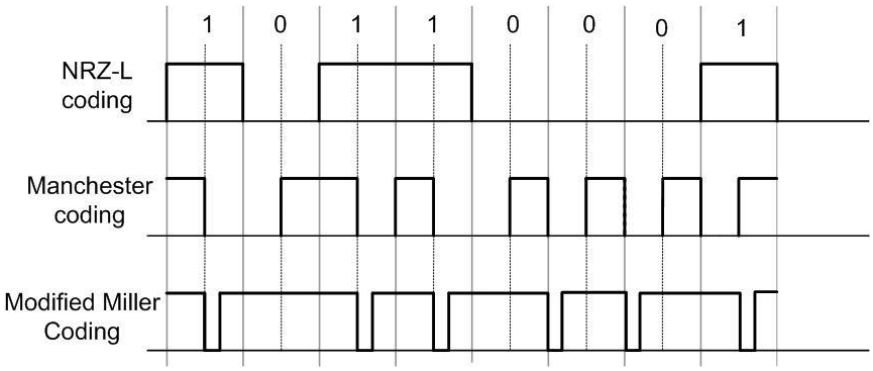

Figure 6: Coding with NFC is either NRZ_L, Modified Miller or Manchester (See also Table 1 and Table 2)

In Figure 7 load modulation is visualized for ASK modulation with Manchester Coding (14443 A PICC or NFC-A device in passive card emulation mode, see 4.2.)

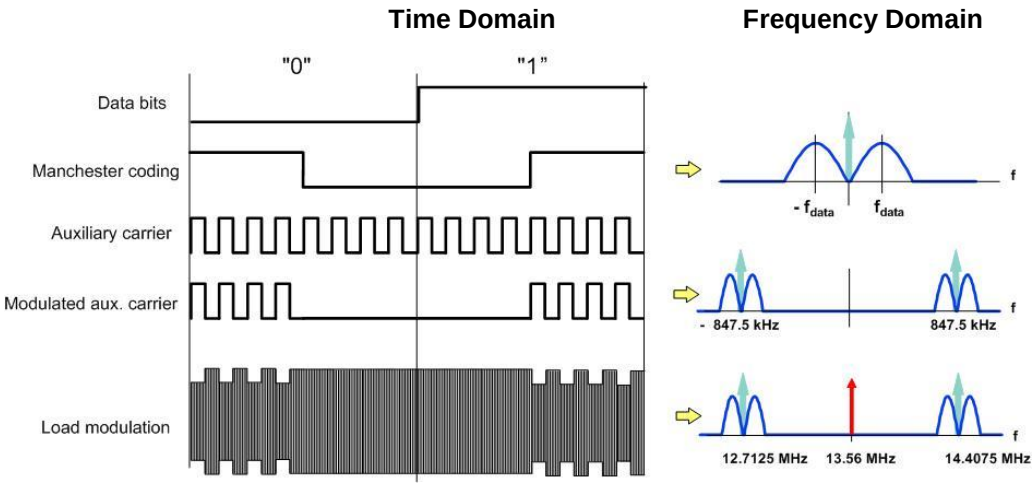

Figure 7: Visualisation of load modulation with auxiliary carrier in time and frequency domain [6]

4 NFC Technology and Signals

4.1 NFC Standards Evolution

The three standards ISO/IEC 14443 A, ISO/IEC 14443 B and JIS X6319-4 are RFID standards which have been prompted by different companies (NXP, Infineon and Sony). The first RF NFC standard was ECMA 340, based on the Air Interface of ISO/IEC 14443A and JIS X6319-4. ECMA 340 was adapted as the ISO/IEC standard 18092. In parallel major credit card companies (Europay, Mastercard, Visa) have introduced the payment standard EMVCo based on ISO/IEC 14443 A and ISO/IEC 14443 B. Within the NFC Forum both groups harmonised the air interfaces. They are named NFC-A (ISO/IEC 14443 A based), NFC-B (ISO/IEC 14443 B based) and NFC-F (FeliCa based).

The evolution of the NFC RF- and protocol standards with its test specifications is shown in Figure 8 and Figure 9.

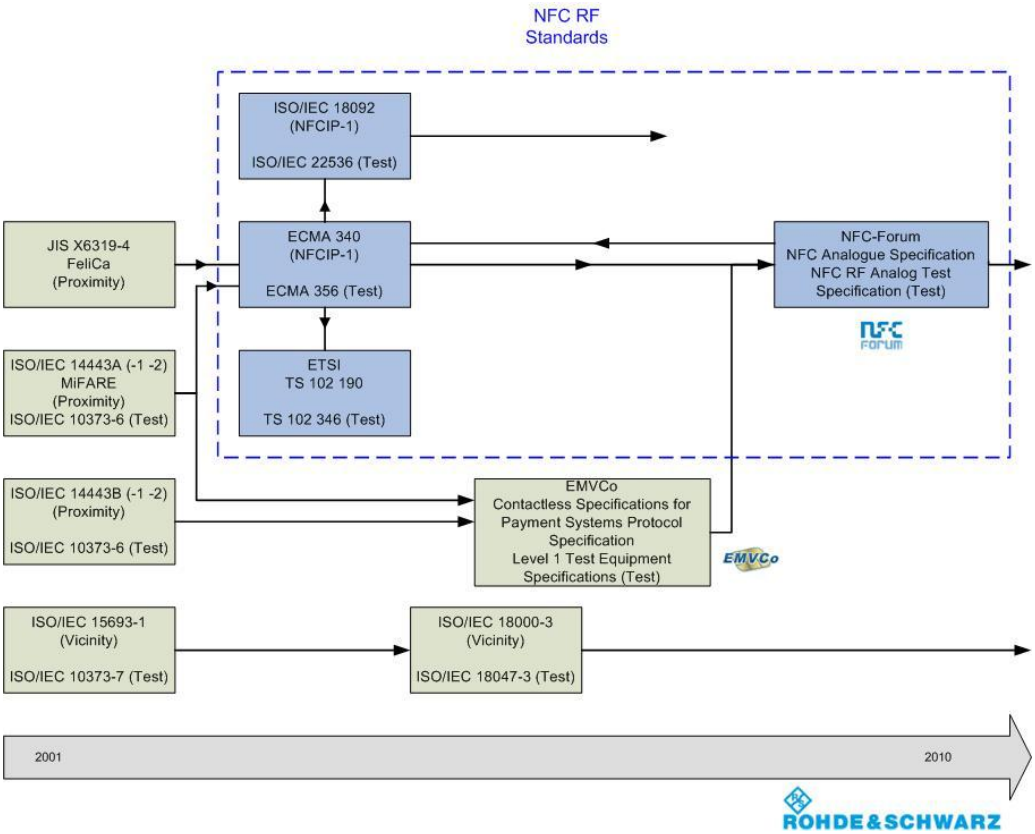

Figure 8: NFC RF standards evolution

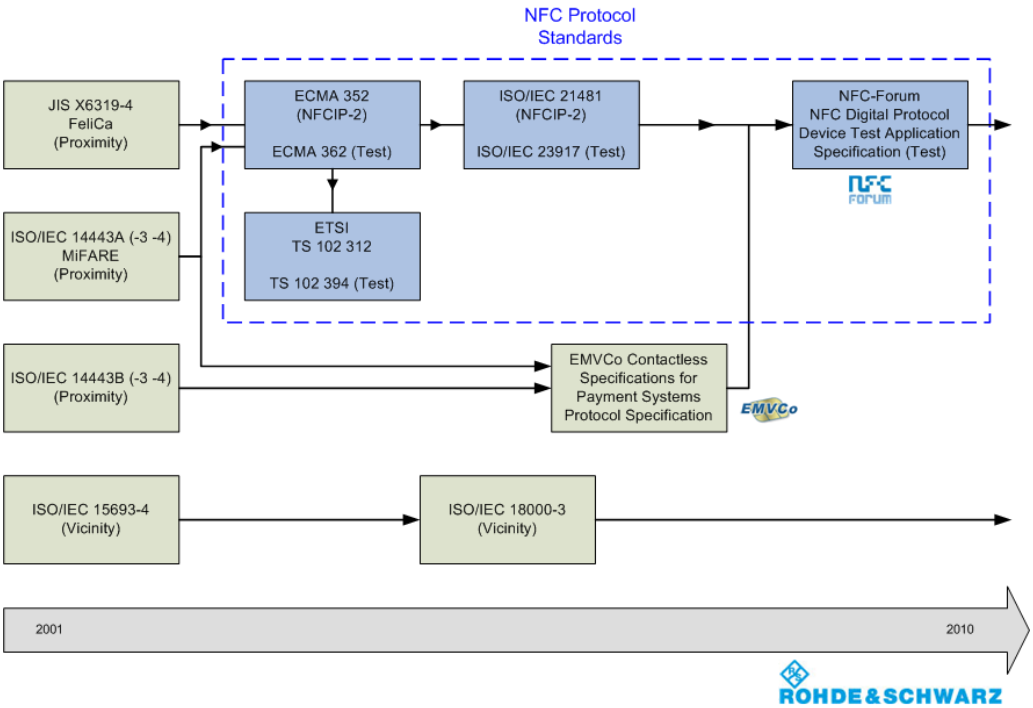

Figure 9: NFC protocol standard evolution

4.2 NFC Operating Modes, Modulation and Coding

There are three main operating modes for NFC:

- Card emulation mode (passive mode): the NFC device behaves like an existing contactless card conforming to one of the legacy standards
- Peer-to-peer mode: two NFC devices exchange information. The initiator device (polling device) requires less power compared to the reader/writer mode because the target (listener) uses its own power supply.
- Reader/writer mode (active mode): the NFC device is active and reads or writes to a passive legacy RFID tag.

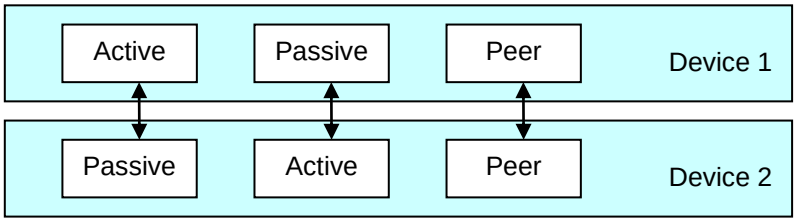

Figure 10: NFC operational modes

Every mode (card emulation, peer-to-peer, reader/writer mode) can be combined with one of the following transmission technologies:

NFC-A (backward compatible to ISO/IEC 14443 A)
NFC-B (backward compatible to ISO/IEC 14443 B)
NFC-F (backward compatible to JIS X 6319-4)

To support all the different technologies, an NFC device in polling mode first attempts to get responses from NFC-A, NFC-B and NFC-F tags with the according request signals. When getting a response from an compatible device, the NFC device sets up the corresponding communication mode (NFC-A, NFC-B or NFC-F mode).

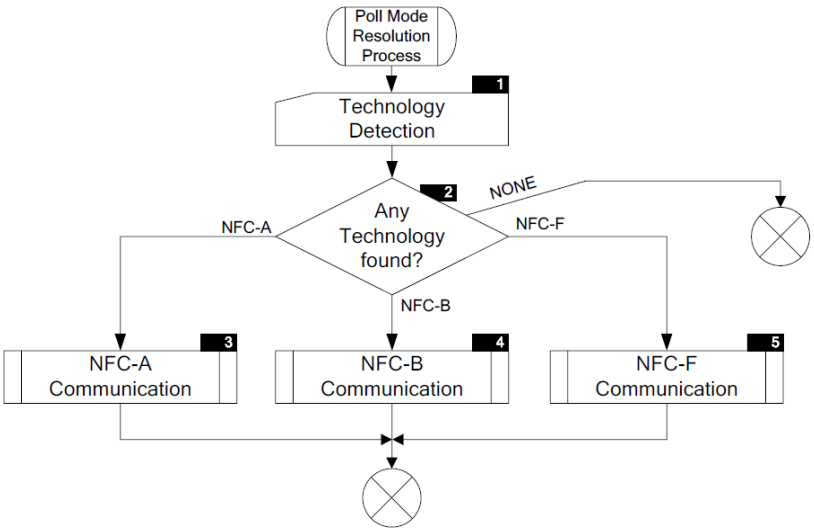

Figure 11: Poll mode resolution process flow chart – main flow [16]

Coding and modulation varies depending on active or passive communication mode, NFC-A, -B, -F communication, and bitrate.
Table 1 shows coding, modulation and data rates for NFC-A, -B or -F communication.

NFC Technical Standards Specifications of the Air Interface					
NFC-Forum Standard	**Polling / Listening**	**Coding**	**Modulation**	**Data Rate**	**Carrier frequency**
NFC-A	Polling	Modified Miller	ASK 100%	106 kb/s	13.56 MHz
	Listening	Manchester	Load modulation (ASK)	106 kb/s	13.56 MHz +- 848 kHz subcarrier
NFC-B	Polling	NRZ-L	ASK 10%	106 kb/s	13.56 MHz
	Listening	NRZ-L	Load modulation (BPSK)	106 kb/s	13.56 MHz +- 848 kHz subcarrier
NFC-F	Polling	Manchester	ASK 10%	212 / 424 kb/s	13.56 MHz
	Listening	Manchester	Load modulation (ASK)	212 / 424 kb/s	13.56 MHz (without subcarrier)

Table 1: NFC RF Standards Overview

4.3 NFC Tag Types

NFC tags are passive devices that can be used to communicate with active NFC devices. The NFC tags are foreseen within applications such as posters, and other areas where small amounts of data can be stored and transferred to active NFC devices. Four basic tag types with designation 1 to 4 each with different format and capacity have been defined. These NFC tag type formats are based on ISO 14443 Types A and B and Sony FeliCa.

NFC Type definition				
	Type 1	**Type 2**	**Type 3**	**Type 4**
ISO/IEC standard	14443 A	14443 A	JIS 6319-4	14443 A / B
Compatible Product	Innovision Topaz	NXP MIFARE	Sony FeliCa	NXP DESFire, SmartMX-JCOP, …
Data rate	106 kb/s	106 kb/s	212, 424 kb/s	106/212/424 kb/s
Memory	96 bytes, expandable to 2 kbyte	48 bytes, expandable to 2 kbyte	Variable, max. 1Mbyte	Variable, max. 32 kbyte
Anti-collision	No	Yes	Yes	Yes

Table 2: NFC tag types

5 NFC RF Measurements

To guarantee the function of NFC devices conforming to the standards as well as comprehensive protocol tests, a number of RF tests also have to be carried out. According to the draft of the NFC Analogue Test Specification [15], (subject to change by the NFC Forum) the RF tests are defined by reference devices (NFC Forum reference listener, NFC Forum reference poller). These reference devices correspond to typical NFC devices in polling and listening mode with different antenna sizes and provide well-defined, comparable measurements.

5.1 Test Setups

The following two test setups are foreseen by the NFC Forum for testing either the listening or the polling mode of an NFC device.

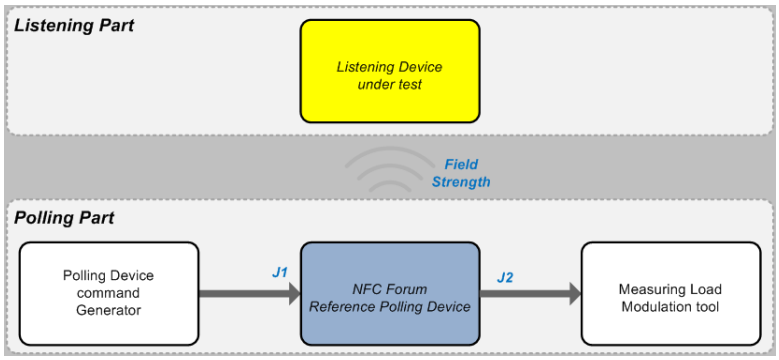

Figure 12: Measurement configuration for testing an NFC device in listening mode [15]

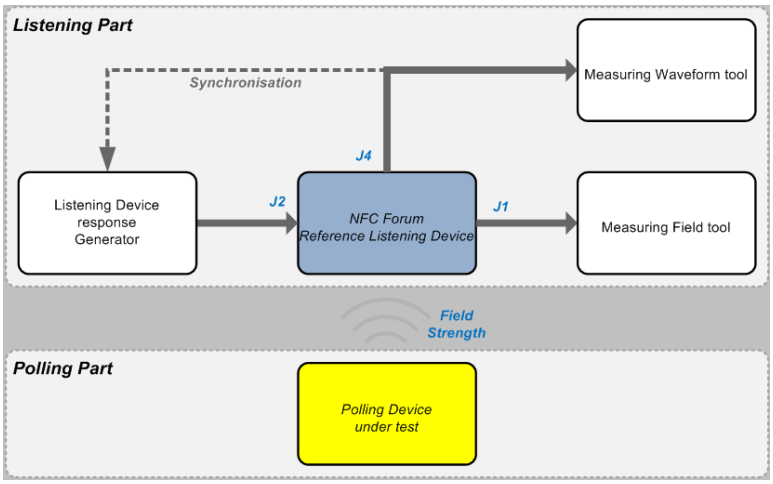

Figure 13: Measurement configuration for testing an NFC device in polling mode [15]

5.2 NFC Forum Reference Devices

Reference Polling Device:

When connected to a suitable signal generator and power amplifier, an NFC Forum reference polling device sends commands to a listening device. The response from a listening device can then be captured and analyzed by measurement equipment.
The NFC Forum reference polling devices with 3 different antenna coil designs are based on the standard EMVCo PCD*) (for Poller-0) and compensated versions of two of the ISO-standardised PICC antenna coil designs (Poller-3 and 6).

*) EMVCo: Europay, Mastercard, Visa Companies [7],
PCD: Proximity Coupling Device (Reader)

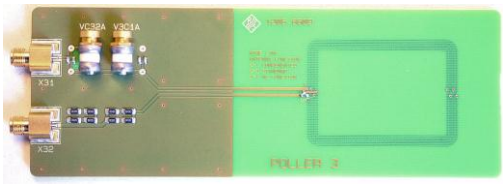

Figure 14: Example: NFC Forum reference poller 3 [15]

Reference Listening Device:

The NFC Forum reference listening device analyses the signal sent out by a polling device. For analyzing the frequency and wave-shapes of these signals, the NFC Forum reference listening device is equipped with an integrated sense coil.
The NFC Forum reference listening device can also send information back to a polling device, using various levels of load modulation generated using an external suitable signal source like an arbitrary waveform generator.

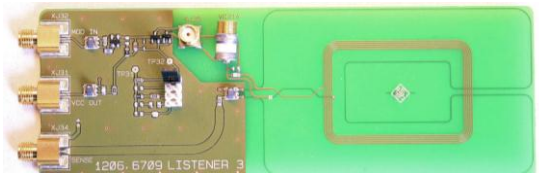

Figure 15: Example: NFC Forum reference listener 3 [15]

The operating volume of a polling device is the space within which the specification requires the device to operate with the aim of ensuring interoperability between NFC devices over at least this volume. The geometry of the operating volume is shown in Figure 16.

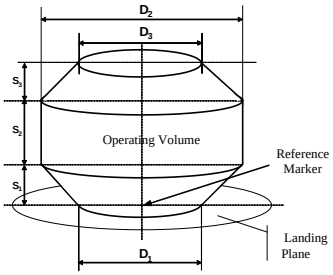

Figure 16: The NFC operating volume is defined as the space in which an NFC Forum device in polling mode can communicate with an NFC Forum device in listening mode or has to be able to communicate with a responding device [15]

5.3 RF Tests on NFC Devices

The RF tests for NFC Forum type approval for NFC enabled devices are specified in the draft NFC Forum Analogue Tests Specification [15]. The most important tests RF tests for an NFC enabled device are basically:

In active polling mode:

- Carrier frequency accuracy measurement
- Power level measurement
  Sufficient power must be delivered in polling mode.
- Waveform characteristics measurement
  Timing parameters like rise-time, fall-time etc. must be checked.
- Load modulation sensitivity test
  The polling device shall correctly receive a load modulation at a minimum specified level.
- Threshold level test (polling device under test shall switch off its RF field when exposed to an external RF field of certain strength).

In passive listening mode:

- Load modulation measurement
  The signal strength of the load modulation (answer of the listener device) must be within required limits.
- Power reception test
  The listening device has to answer correctly even in bad conditions.
- Frame Delay Time (important in NFC-A mode for the anti-collision-algorithm)
  The Frame Delay Time is the response time from the end of the polling command to the start of transmission of the phone in card emulation mode.

All these tests are to be carried out for the different modes NFC-A, NFC-B und NFC-F if supported by the mobile phone.

Basic tests of NFC enabled devices are described in detail in the R&S Application Note 1MA190 “Basic Tests of NFC Enabled Devices Using R&S Test Equipment” [17].

Abbreviations

Abbreviations	
Abbreviation	**Description**
ASK	Amplitude Shift Keying
BPSK	Binary Phase Shift Keying
NRZ-L	Non-Return to Zero, (L for Level)
OOK	On-Off-Keying
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
ECMA	European Association for Standardizing Information and Communication Systems
EMVCo	EMVCo Europay, Mastercard, Visa Companies. EMVCo manages, maintains and enhances the EMV® Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo is currently owned by American Express, JCB, MasterCard and Visa
JIS	Japanese Industrial Standard
NFC	Near Field Communication
NFC-A	Near Field Communication – NFC-A Technology
NFC-B	Near Field Communication – NFC-B Technology
NFC-F	Near Field Communication – NFC-F Technology
NFCIP-1	Near Field Communication Interface and Protocol according to *[NFCIP-1]*. Specific protocol of the NFC Peer Mode
NDEF	NFC Data Exchange Format
PCD	Proximity Coupling Device (Reader)
PICC	Proximity Integrated Circuit Card

6 Literature

[1] Klaus Finkenzeller, “RFID Handbuch”, Hanser Verlag
[2] Josef Langer, Michael Roland “Anwendung und Technik von Nearfield Communication (NFC)”, Springer Verlag
[3] http://www.nfc-forum.org/home/
[4] Keen: NFC Forum Technical Overview. Slides (April 2009)
[5] NFCForum-CS-DeviceTestApplication-1.1
[6] RFID – Protokolle, Vorlesung RFID Systems, Michael Gebhart, TU Graz
[7] http://www.emvco.com
[8] ISO/IEC 14443-2 Identification cards-Contactless integrated circuit cards-Proximity cards – Part 2: Radio frequency and signal interface
[9] JIS X6319-4 (2005) Specification of implementation for contactless circuit card(s)-Part 4: High Speed proximity cards
[10] Standard ECMA-340 Near Field Communication Interface and Protocol (NFCIP-1)
[11] ETSI TS 102 190 Near Field Communication (NFC) IP-1;Interface and Protocol (NFCIP-1)
[12] ISO/IEC 18092 Information technology-Telecommunications and information exchange between systems-Near Field Communication-Interface and Protocol
[13] EMV Contactless Communication Protocol Specification
[14] NFC Digital Protocol Technical Specification 1.0
[15] NFC Analogue Specification Draft, Technical Specification, NFC ForumTM (Subject to change by the NFC Forum)
[16] NFCForum-CS-Device Test Application 1.1
[17] Application Note 1MA190 “Basic Tests of NFC Enabled Devices Using R&S Test Equipment”

About Rohde & Schwarz
Rohde & Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde & Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability
- ISO 14001-certified environmental management system

Certified Quality System
ISO 9001

Regional contact

Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1-888-TEST-RSA (1-888-837-8772)
customer.support@rsa.rohde-schwarz.com

Latin America
+1-410-910-7988
customersupport.la@rohde-schwarz.com

Asia/Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

This application note and the supplied programs may only be used subject to the conditions of use set forth in the download area of the Rohde & Schwarz website.

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG; Trade names are trademarks of the owners.

Rohde & Schwarz GmbH & Co. KG
Mühldorfstraße 15 | D - 81671 München
Phone + 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

www.rohde-schwarz.com