NFC SmartTool

Reference Manual

ipTronix
Via Aurelia, 1051
00166 Rome, Italy
Tel. +39 06 66183814
Fax +39 06 66188420
EMail: info@iptronix.com
Web: www.iptronix.com

Rev: 2
Date: 12/06/2014
Classification: Public

Trademarks

Visit our web page at www.iptronix.com
For support requests, contact us at support@iptronix.com
For documentation suggestions, corrections, or requests, contact techpubs@iptronix.com

Revision History

Revision	Date	Description
0	14/10/2013	First Release
1	3/12/2013	Updated LPCXpresso installation information
2	12/06/2014	Updated note on LPC-Link2 JTAG connection

1 Overview

Document Scope

Scope of this document is to help approach to contactless identification and information exchange through Mifare and NFC.

Document Purpose

This document describes the ipTronix/Arrow/NXP reference design with a number of different applications that can be quickly and easily run on the SmartTool demo board, to demonstrate various usage scenarios of NFC technologies.

References

[1] http://code.google.com/p/libnfc/
[2] http://www.nfc-forum.org/home
[3] http://www.nfc-forum.org/specs/spec_list/#protts
[4] http://www.commoncriteriaportal.org/.
[5] http://ridrix.wordpress.com/2009/09/19/mifare-desfire-communication-example/
[6] http://www.nearfieldcommunication.org/nfc-signaling.html
[7] http://www.nfc-forum.org/resources/white_papers/Innovision_whitePaper1.pdf
[8] http://www.open-nfc.org
[9] http://developer.nokia.com/Develop/NFC/Documentation/
[10] http://www.nfc-forum.org/aboutnfc/interop/
[11] http://www.nfc-forum.org/specs/spec_dashboard/
[12] http://learn.adafruit.com/adafruit-pn532-rfid-nfc/ndef
[13] http://www.nxp.com/redirect/nfc-forum.org/specs
[14] AN1445 Antenna design guide for MFRC52x, PN51x, PN53x; AN1444 RF Design Guide including Excel Calculation sheet (http://www.nxp.com/search?q=an1445_an1444&type=keyword&rows=30)
[15] http://www.ti.com/rfid/docs/manuals/appNotes/HFAntennaDesignNotes.pdf
[16] http://www.gorferay.com/tuning-procedure-with-oscilloscope/
[17] http://read.pudn.com/downloads153/doc/670844/Design_of_MF_RC500_Matching_circuits_and_Antennas.pdf

Notes

Providing detailed information about the components used in the reference design is out of the scope of this document. Data sheets, documents and application notes for components, software and used tools are available on the following web sites:

- http://www.nxp.com/demoboard/OM13054.html
- http://www.lpcware.com/content/project/freertos-nxp-m0-m3-and-m4-mcus
- http://www.lpcware.com/lpcxpresso/home
- http://lpcxpresso.code-red-tech.com/LPCXpresso/
- http://www.code-red-tech.com/RedSuite5/red-suite-5-nxp.php
- http://www.freertos.org/
- http://www.freertos.org/FreeRTOS-for-Cortex-M0-LPC1114-LPCXpresso.html

Although this document describes some of the underlying technologies, it is not intended to be a complete reference for Mifare and NFC standards, hence the reader is expected to have at least some background on these topics.

For detailed information on NFC and Mifare standards please refer to the following web sites:
http://www.nfc-forum.org/home/
http://www.mifare.net/

Definitions, Symbols and Acronyms

Definitions

Symbols

Acronyms

AES	Advanced Encryption Standard
AID	Application Identifier
AMK	Application Master Key
AN	Application Note
APDU	Application Protocol Data Unit
DES	Data Encryption Standard. Single key and single cryptographic process
3DES	A DES operation using 2 keys and a three stage cryptographic process
3k3DES	A DES operation using 3 keys and a three stage cryptographic process
FID	File IDentifier
FPGA	Field Programmable Gate Array
GPIO	General Purpose Input/Output
JTAG	Joint Test Action Group
HMI	Human-Machine Interface
ICC	Integrated-Circuit Card. (This is the standard name for a plastic card holding a silicon chip (an integrated circuit) compliant with the ISO 7816 standards. A common name is smartcard).
LSB	Least Significant Byte
LSb	Least Significant Bit

LCD	Liquid Crystal Display
MAC	Message Authentication Code
MAD	Mifare Application Directory
MCU	Micro Controller Unit
MSB	Most Significant Byte
MSb	Most Significant Bit
NDEF	NFC Data Exchange Format
NFC	Near Field Communication
NRND	Not Recommended for New Design
NUID	Non-Unique Identifier
PCB	Printed Circuit Board
PCD	Proximity Coupling Device (“Contactless Reader”). (This is the standard name for any contactless card compliant with the ISO 14443 standards).
PICC	Proximity Integrated Circuit (“Contactless Card”). (This is the standard name for any contactless card compliant with the ISO 14443 standards).
PKE	Public Key Encryption (like RSA or ECC)
RF	Radio Frequency
RFID	Radio-Frequency Identification.
RFU	Reserved For Future Use
SIM	Subscriber Identity Module
SAM	Secure Authentication Module
TLV	Tag, Length, Value
UI	Uman Interface
UID	Unique Identifier, also called serial number in the [MF1K, MF4K, MFPLUS] specification
USID	Unique Services Identifier
VCD	Vicinity Coupling Device (a device able to communicate with a VICC, i.e. a contactless reader compliant with ISO 15693).
VICC	Vicinity Integrated Circuit Card (This is the standard name for any contactless card compliant with the ISO 15693 standards (vicinity: less than 150cm). Common names are RFID tag, RFID label).

Number representation

The following conventions and notations apply in this document unless otherwise stated.
Decimal numbers are represented as is (without any tailing character) (example: 245).
Binary numbers are represented by strings of 0 and 1 digits shown with the most significant bit (MSb) left and the least significant bit (LSb) right, “b” is added at the end (example: 11110101b).
Hexadecimal numbers are represented using the numbers 0 - 9 and the characters A – F, with a trailing “h”. Sometimes number is prefixed with “0x” and no trailing symbol is added.
The Most Significant Byte (MSB) is shown on the left, the Least Significant Byte (LSB) on the right (example: F5h or 0xF5).

Terms and Definition

According to the NDEF specification, data is represented in Network Byte Order (i.e.big endian). This means Most Significant Byte first and most significant bit first (MSB first, msb first).
Please note that the MIFARE DESFire EV1 is using the LSB first notations for APDU communication.

2 Introduction

This reference design can be used as a base to design a low cost system applicable to access control, security, micro payment and contactless information exchange between a smartphone and a custom machine.
Components of the design are a microcontroller demo board (the SmartTool demo board), the embedded source code (board drivers, libraries and applications) and an Android application to demonstrate NFC communication.

Since the Crypto1 algorithm (used on MIFARE card) has been violated, NXP recommends the newer and more secure Mifare DESFire cards for applications where security is critical.

Note

This reference design is only for demonstration purposes and is not guaranteed to comply with EMI or other compliance requirements.
This reference design does not replace any relevant RF design documents and it does not cover EMC related topics.

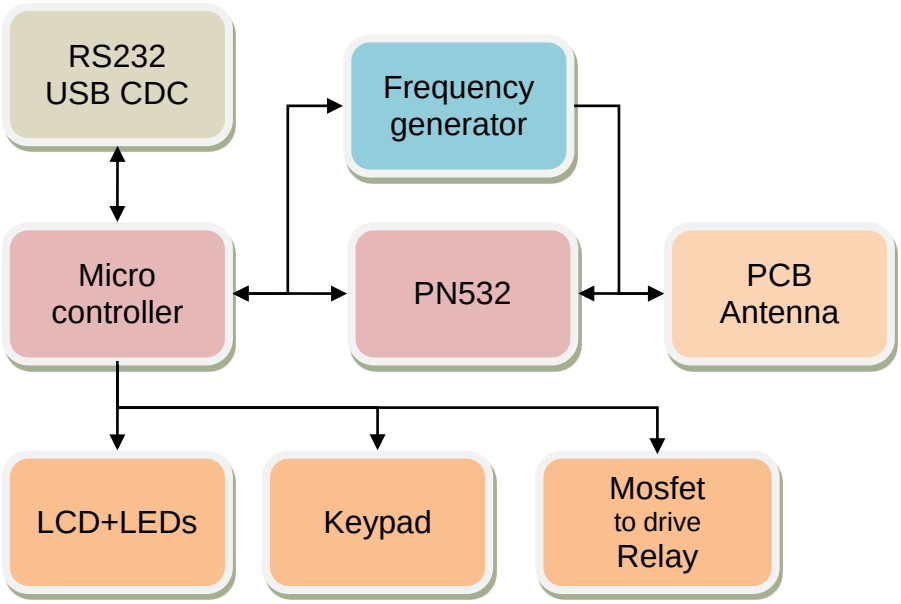
Note on Antenna PCB

NFC is intended for short range applications, hence card detection distance is in the order of few cm. it is strongly recommended to test the antenna design in the final mechanical assembly as any metallic part close to the antenna can alter its performance and detection distance.

3 General Description

System architecture

The demo board uses a PN532 device controlled by a NXP Cortex M0 microcontroller (LPC11U37) running a customized port of libNFC [1]. The Cortex M0 is a low power, low cost processor, still having the necessary computational power for the purpose.
The block diagram below shows the system's main components; a number of peripherals such as capacitive keypad, LCD, LEDs and relay are provided to allow demonstration of a real world access control as well as micro payment applications.



An optional frequency generator has also been added as a tool for customers to easily tune their PCB antennas, which is one of the biggest pitfalls in NFC/Mifare designs. The released software contains an application specifically made for this purpose. Running this application the customer can verify the performance of the embedded antenna or use the board as a tool to verify the performance of a different antenna.

Reference embedded applications

This reference design includes several production ready applications that demonstrate card reader/writer, card emulation and NFC functionality.

In case of dual role (reader/card emulation) the software alternatively polls the cards for a programmable time and then switches to card

emulation in order to be read by cell phones. Note that since cell phones have a polling time that can be over 1 sec it is recommended to have card emulation last at least 1.5 sec in order to ensure reliable detection.
For card emulation the chosen method is to emulate a type 4 NFC tag (memory size up to 32Kbytes, communication speed 106Kbit/sec) with the possibility to read and write information to/from a NFC enabled smartphone.

Type 4 NFC tag emulation is the recommended way to communicate with a smartphone as it allows easy bidirectional communication and implements a standard way of exchanging a wide amount of data. This approach for example allows to provide the smartphone with a URL that points to the application required, if that application has not yet been installed, and at the same time allows to provide data to the application if it is already installed (by using smart poster NDEF records). The application can in turn write a response to the emulated tag for example to authenticate itself for access control applications.

Mifare/DESFire tag read/write is used to allow secure access to data such as personal information or credit for micro payments. The flexibility of Mifare/DESFire tags allows multiple vendors to store in the same tag proprietary, encrypted data that can be accessed only with valid passwords. This means that the same tag can contain for example workout training schedule, coffee machine credit and access authorizations to secure areas of a building.

The dual role is implemented by switching between these two working modes at fixed timing intervals thus allowing the same device to support both smartphones and passive tags.

In order to allow customer to easily use single or dual role, several examples are provided in the software package.

Note that peer to peer protocols such as SNEP or NPP have not been ported due to the limited memory footprint of the cortex-M0. On bigger devices it may be possible to port such functionality but the ease of implementation of data exchange with phones through type 4 card emulation makes this overkill.

Supported Cards

Provided software is compatible with Mifare UL, Mifare Classic and DESFire cards. Mifare UL cards are the cheapest but offer little space and no security; Mifare classic offer up to 4K with password protection (although security has been violated) but some mobile phones are not compatible with them. DESFire cards are fully supported on all phones however security part is not natively supported by OS vendors.

LibNFC customizations

In order to run on small microcontrollers libNFC requires customizations to reduce memory footprint and reduce the need for heap management APIs (malloc/free) which are usually a source of malfunctions in memory constrained systems.
This reference design makes use of a customized version of libNFC that implements a number of optimizations such as:

- Reduced number of malloc/free calls
- Better handling of logging and debugging features in order to remove redundant code and eliminate printfs with a compilation switch
- Abstraction of low level functions such as delay, logging and communication to allow easy porting on other platforms

Android app

In order to demonstrate functionality with Type 4 tags an android app that allows exchanging data with the tag has been developed. Since data exchange is not encrypted, it is developer's responsibility to ensure security by encrypting data through adequate methods.

Antenna calibration Application

According to NXP reference designs, in order to correctly calibrate the PCB antenna, it is necessary to measure the parameters of the antenna with networks analyzers that seldom are available at customer's labs. A more straightforward approach is proposed here, where a provided application makes use of the on board frequency generator to feed the antenna with a frequency sweep around the desired resonance frequency. At the same time the microcontroller reads the peak amplitude of the signal on the antenna and samples it with the internal ADC, showing a frequency response diagram that can be used to tune compensation network.
With this simple tool the customer will be able to quickly identify tuning components needed to adjust the resonance frequency with a trial and error procedure that would be required in any case, but without the need of expensive equipment.

Documentation

This reference design is completed with documentation on APIs and hints on porting and creation of user applications, showing hooks where the application can be customized or eventually points where the demo application can be spliced to be inserted in other existing systems.

In addition to full source code for applications and libraries both for embedded and android systems, hardware documentation is provided in OrCAD Capture, PADS PCB and gerber formats with production ready design files.

4
Introduction to NFC

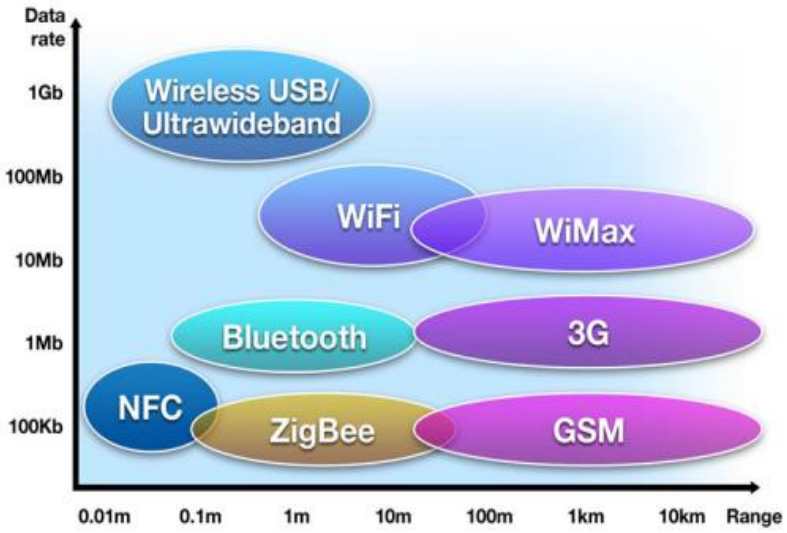
The Near field communication (NFC) is a radio technology that enables communication between devices without direct physical touch.

NFC is based on and extends RFID (Radio Frequency Identification) and operates on 13.56 MHz frequency with distance range between devices up to 10 cm. It supports 3 operating modes, Peer-to-Peer, Card Emulation, Read/Write, and different data transmission rates such as 106, 212, and 424 kbps.

.

The following diagram shows a brief comparison of range distance between several low power wireless technologies

(Information of difference standards is available on internet).



A quick comparison between NFC and others short-range communication technologies is show below:

	NFC	RFID	IrDA	Bluetooth
SET-UP TIME	< 0,1ms	< 0,1ms	~ 0,5s	~ 6 s. (~ 1 s. if Low Energy)
RANGE (theoretical)	Up to 10 cm	Up to 3 m	Up to 5 m	Up to 30 m (10 m low energy)
***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

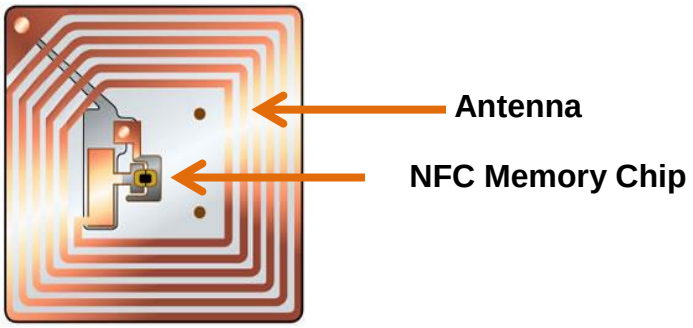
Comparing NFC to other close range communication technologies (Source: NFC Forum [2])

Since NFC is an open-platform technology, more information is available on NFC Forum website [2]. The NFC Forum is a non-profit industry association formed on 2004, by NXP Semiconductors (spin off from Philips Electronics in 2006), 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. Currently there are 4 working groups, one of which dedicated to security.

The Tag and the reader:

NFC-based communication between two devices is possible when one device acts as a reader/writer and the other as a tag.

- The tag (for example stickers or wristbands) is a simple passive device , powered by magnetic field, containing antenna and small memory chip that can be read only, re-writable, and writable once.



- The reader is an active device, which generates radio signals to communicate with the tags. In case of passive mode of communication, the reader powers the passive device.

Tag types

To guarantee interoperability, file systems have been standardized.
NFC forum defines 4 types of standard tags: Type 1 tags, Type 2 tags, Type 3 tags, Type 4 tags.

#	NFC Forum Platform	Compatible Products
1	NFC Forum Type 1 Tag	Innovision Topaz
2	NFC Forum Type 2 Tag	NXP Mifare Ultralight NXP Mifare Ultralight C
3	NFC Forum Type 3 Tag	Sony FeliCa
4	NFC Forum Type 4 Tag	NXP DESFire NXP SmartMX with JCOP or other compatible contactless products

Type MIFARE Classic has been defined by NXP and is only optionally supported not being part of NFC forum specification.

The specifications for the tag types are available for free from the NFC-Forum website.

Comparison of the different product compatible with the NFC Forum (Type Tag) Platform and the NXP Specific (Type Tag) Platform

	NFC Forum Platform				NXP Specific Platform
	Type 1 tags	**Type 2 tags**	**Type 3 tags**	**Type 4 (A or B) tags**	**Type MIFARE Classig Tag**
Technology	NFC-A	NFC-A	NFC-F	NFC-A NFC-B	NFC-A
Standard	ISO-14443A	ISO-14443A	Japanese Industrial Standard (JIS) X 6319-4 ISO18092	ISO-14443A ISO-14443B	ISO-14443A
Data Access	Read and re-write capable, users can configure the tag to be read-only	Read and re-write capable, also users can configure the tag to be read-only	Pre-configured at manufacture to be either read and re-writable, or read-only	Pre-configured at manufacture to be either read and re-writable, or read-only	Read and re-write capable, also users can configure the tag to be read-only.
Memory (bytes)	96 to 512	48 to 2K	up to 1 M per service	up to 32 K per service	192 / 768 / 3584
Communication speed (Kbits/s)	106	106	212 or 424	106 or 212 or 424	106
Data collision protection	No	Yes	Yes	Yes	Yes
Compatible products available in the market	Innovision Topaz, Broadcom BCM20203	NXP MIFARE Ultralight	Sony FeliCa	NXP Mifare DESFire, SmartMX-JCOP	NXP MIFARE Classic 1k, MIFARE Classic 4K, and Classic Mini
Unit Price	Low	Low	High	Medium / High	low

Additional information is available by visiting [3]

Mifare Products Family

The MIFARE name covers proprietary technologies of NXP (spin off from Philips Electronics in 2006) based upon various levels of the ISO/IEC 14443 Type A 13.56 MHz contactless smart card standard.

With MIFARE word is identified not a single product but rather a family of devices from NXP Semiconductors

	MIFARE Ultralight MF0 U10 MFO U11	**MIFARE Ultralight C** MF0 U20 MF0 U21	**MIFARE Classic** MF1 S20 MF1 S50 MF1 S70	**MIFARE Plus** MF1 S61 MF1 S71	**MIFARE DESFire(EV1)** MF3 D21 MF3 D41 MF3 D81
HW Crypto	-	3DES	Crypto 1	Crypto 1, AES	3DES, AES
EEPROM	512 Bit	1536 Bit	320B,1KB,4KB	2,4 Kbyte	2,4,8 Kbyte
Special Features	-	Anti-Cloning function	-	MIFARE Classic Compatible	-
Certifications	-	-	-	CC EAL 4+	CC EAL 4+
Contactless Interface	ISO 14443 A (13.56MHz, up to 10cm distance, 106 - 848kBaud)				

	MIFARE Mini MF1 S20	**MIFARE Ultralight C** MF1 S50	**MIFARE Plus 2K** MF1 S61	**MIFARE 4K** MF1 S70	**MIFARE Plus 4K** MF1 S71
HW Crypto	Crypto 1	Crypto 1	Crypto 1, AES	Crypto 1	Crypto 1, AES
EEPROM	320 Byte	1024 Byte	2048 Byte	4096 Byte	4096 Byte
Special Features	-	-	MIFARE 1K Compatible	MIFARE Classic Compatible	MIFARE 4K Compatible
Certifications	-	-	CC EAL 4+		CC EAL 4+
Contactless Interface	ISO 14443 A (13.56MHz, up to 10cm distance, 106 - 848kBaud)				

Abbreviations information:

3DES = The Data Encryption Standard (DES) is a previously predominant algorithm for the encryption of electronic data.
AES= The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES has been adopted by the U.S. government and is now used worldwide.
Crypto 1 = Crypto1 is a proprietary encryption algorithm @ 48 bits created by NXP Semiconductors specifically for Mifare RFID tags.

CC EAL 4+ = The Common Criteria for Information Technology Security Evaluation (abbreviated as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification.
More information on [4]

Since the algorithm Crypto1 has been violated, NXP recommends using Mifare DESFire in applications where communications security is critical.

MIFARE DESFIRE

MiFare DESFire are iso14443A compliant contactless smartcards, and support all layers including iso14443-4. These cards are so-called “stored value” cards, so you cannot install and execute your own program code on DESFire cards.
DESFire is like a memory card with access control (typical usage is within public transportation and access control).
DESFire cards are considered secure. Even though there are some theoretical security flaws, unlike Mifare classic cards, no public working hack has been published. Note that the new DESFire EV1 cards are supposed to address the flaws found in v0.6.
Depending on card version a DESFire card might support commands in native, native-wrapped or iso7816-4 command set styles.

- Software version v0.4 does not support APDU (only native commands)
- v0.5 adds support for wrapping native commands inside ISO 7816 style APDUs
- v0.6 adds ISO/IEC 7816 command set compatibility.

New DESFire cards versions (EV1) (v1.3) support extended APDU commands.
See [5] for more information.

Mifare DESFire EV1

MIFARE DESFire EV1 is based on open global standards for both air interfaces and cryptographic methods.
It is compliant to all four levels of ISO / IEC 14443 A and uses optional ISO / IEC 7816-4 commands.
Featuring an on-chip backup management system and the mutual three pass authentication, a MIFARE DESFire EV1 card can hold up to 28 different applications and 32 files per application.
The size and access conditions of each file are defined at creation time.
MIFARE DESFire EV1 uses a DES, 2K3DES, 3K3DES and AES Hardware cryptographic engine for securing transmission data.

NFC Signaling Technologies

Three different signaling technologies coexist within the NFC standard and when a reader and a tag come in proximity, they first have to exchange information on what technology they support in order to agree on the physical communication protocol.

NFC-A (Type A)
NFC-A corresponds with RFID Type A communication. In Type A communication, Miller encoding, also known as delay encoding, is used with amplitude modulation at 100 percent. Using this set-up, a signal sent between devices must change from 0 to 100 percent to register the difference between sending a “1” and a “0.” Data is transmitted at 106 Kbps when using Type A communication.
NFC-B (Type B)
Similar to NFC-A, NFC-B corresponds with RFID Type B communication. Instead of Miller encoding, Type B uses Manchester encoding. Amplitude modulation is at 10 percent, meaning a 10 percent change from 90% for low to 100% for high is used. A change from low to high represents a “0” while high to low represents a “1.”
NFC-F (Type F)
NFC-F refers to a faster form of RFID transmission known as FeliCa. Commly found in Japan, FeliCa is a technology similar to NFC but faster and currently more popular. It is used for a variety of services such as subway tickets, credit card payments, and identification at office buildings and other locations with limited access.

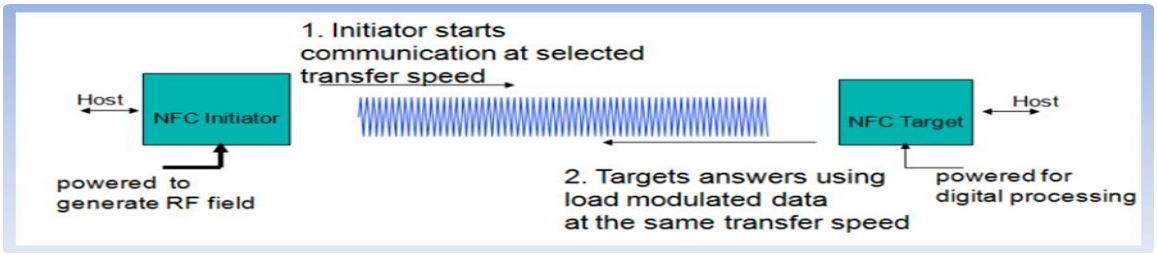
More information can be found on [6].

NFC Communication modes

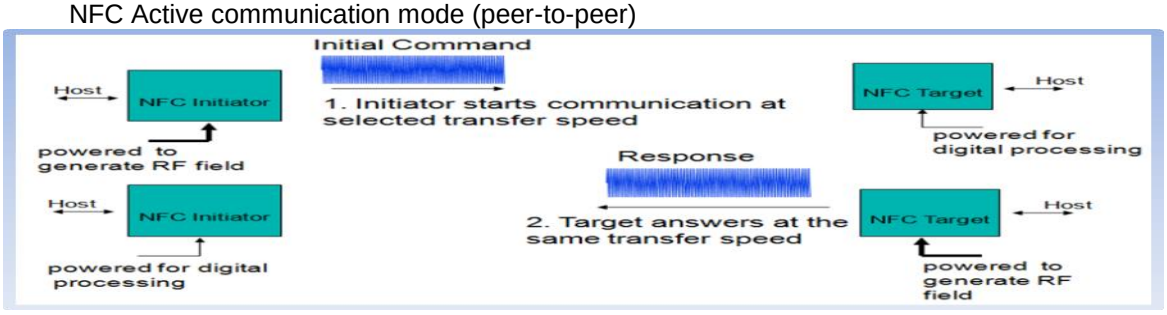
NFC devices support two communication modes :

- Active mode: the target and the initiator devices have power supplies and can communicate each other by alternate signal transmission (peer-to-peer).
- Passive mode**:** the initiator device generates radio signals and the target device is powered by this electromagnetic field. The target device responds to the initiator by modulating the existing electromagnetic field.

NFC Passive communication mode



NFC Active communication mode (peer-to-peer)



Operation modes

NFC devices can operate in three different modes based on the ISO/IEC 18092, NFC IP-1 and ISO/IEC 14443 contactless smart card standards.

- **Read / Write**

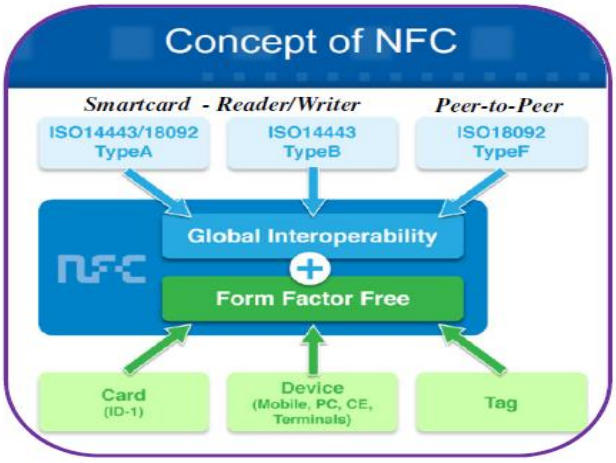
  In this mode, the NFC enabled device can read or write data to any of the supported tag types in a standard NFC data format.

- **Peer to peer**

  In this mode, two NFC-enabled devices can exchange data. For example, you can share Bluetooth or Wi-Fi link set up parameters to initiate a Bluetooth or Wi-Fi link. You can also exchange data such as virtual business cards or digital photos. Peer-to-Peer mode is standardized in the ISO/IEC 18092 standard.

- **Card emulation**

  An NFC-enabled device acts as reader when in contact with tags. In this mode, the NFC device can act as a tag or contactless card for existing readers.



Protocol stacks & Standards overview

The underlying layers of NFC technology are ISO, ECMA and ETSI standards.
Since NFC is compliant with the main international standard for smartcard interoperability (ISO 14443), it is compatible with the millions of contactless smartcards and readers already in use worldwide.
nfc_innovision_7
The communication protocols between NFC devices are defined (in the same way) in ISO, ECMA and partially also in ETSI standards.
The main ones are:

- Near Field Communication interface and protocol (NFCIP-1)
  (ETSI TS 102.190, ISO/IEC 18092, ECMA 340)

Standardizes RF field/signal interface, initialization/anti-collision, transport protocols, Active and passive RF modes, peer-to-peer mode, several data rates

- Near Field Communication interface and protocol (NFCIP-2) (ISO/IEC 21481, ECMA 352)
  Defines selection mechanism between different contactless technologies (operating at the same frequency of 13.56 MHz); It is intended to be used by mobile devices that support communication according to ISO 18092(NFCIP-1), ISO/IEC 14443, but they will be also compatible with other contactless standards like ISO/IEC15693

In June 2006, the NFC Forum introduced standardized technology architecture, initial specifications and tag formats for NFC-compliant devices. These include Data Exchange Format (NDEF), and three initial Record Type Definition (RTD) specifications for smart poster, text and Internet resource reading applications.
In addition, the NFC Forum announced the initial set of four tag formats that all NFC Forum-compliant devices must support. These are based on ISO 14443 Types A and B (the international standards for contactless smartcards) and FeliCa (derived from the ISO 18092, passive communication mode standard).
Tags compatible with these mandatory formats are available initially from Innovision, Philips, Sony and other vendors, and more than one billion tags are already deployed globally.
The NFC Forum chose the initial tag formats to cater for the broadest possible range of applications and device capabilities

Relevant specifications for smart cards and Read/write are:

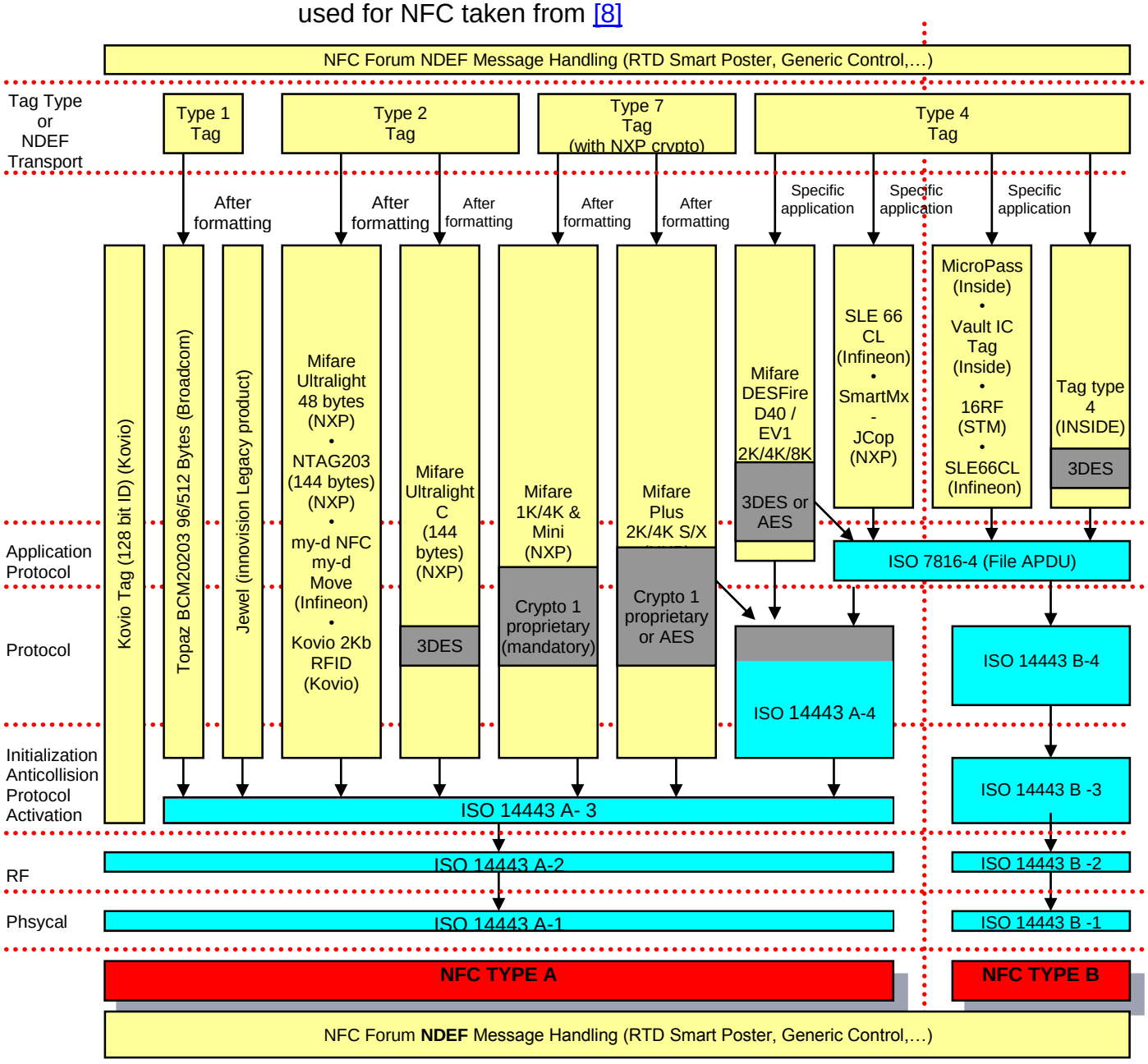
- ISO14443–3: Defines how tags are discovered, how anti-collision is managed if >1 tag, and how tag type is identified („SAK byte“). Available in 2 flavors A and B
- ISO14443–4: defines APDU protocol (ISO 7816) over contactless interface
- NFC Data exchange Format (NDEF): standard content format for URIs, etc…
- Type 1&2 use proprietary protocols on top of ISO14443-3 (Tags by Innovision and NXP)
- Type 3 (Felica unsecure) is using an entirely proprietary protocol defined by Felica

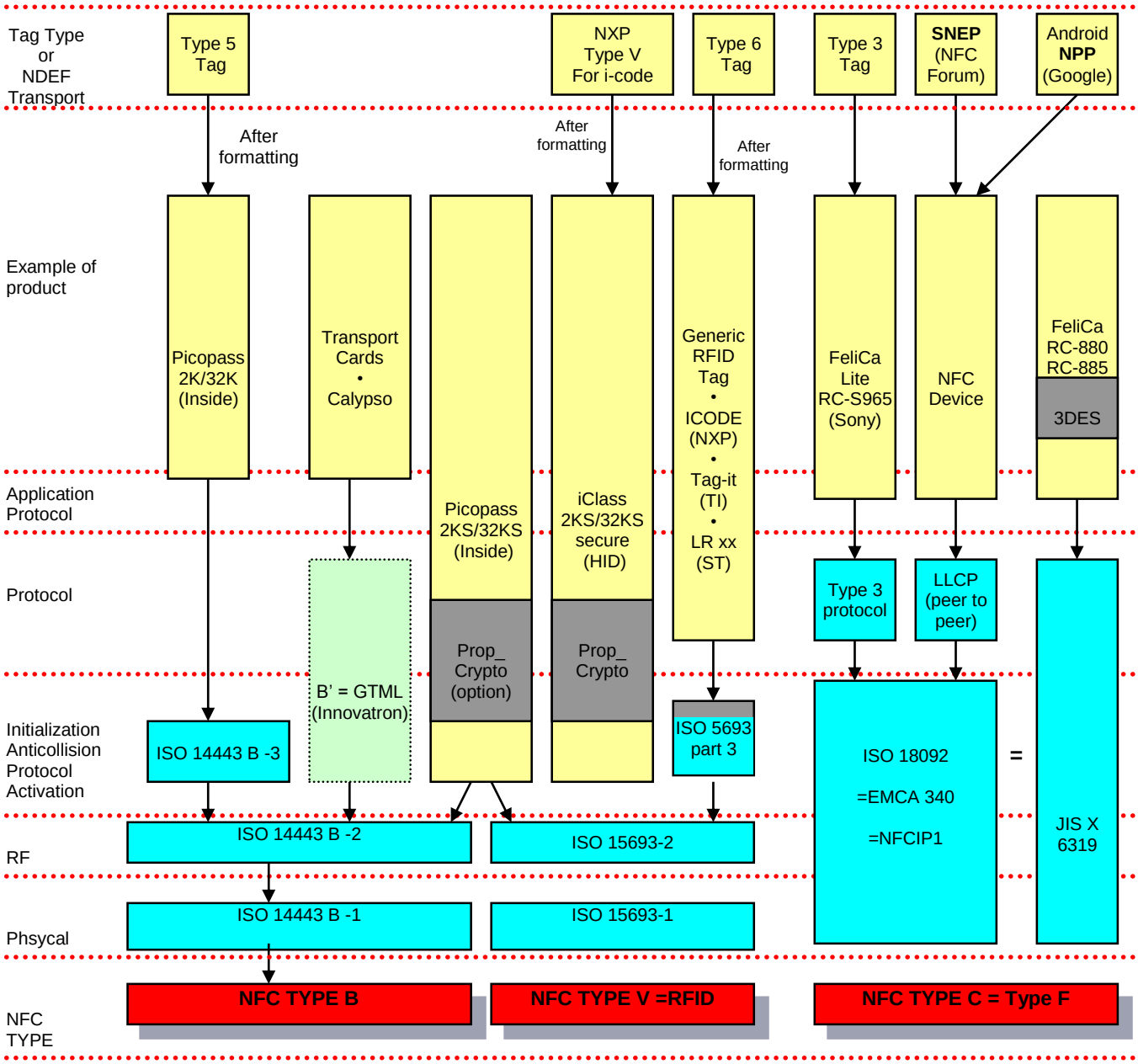
Relevant specifications for P2P (Peer to Peer)

- NFCIP 1 (ISO/IEC 18092) – NFCIP-1: borrowing from ISO14443-3 (106 kbit/s) and JIS X 6319 (212, 424kbit/s) plus a simple data exchange protocol (DEP) for P2P on top
- Logical Link Control Protocol (LLCP): smooth establishment of communication. (e.g. handles Initiator + Target Configuration, flow control, …)
- Simple NDEF Exchange Protocol (SNEP): exchange NDEF messages over LLCP.

- NFC forum may define other bindings of existing protocols (like OBEX)

The following picture shows a diagram of most protocols and standards used for NFC taken from [8]





For additional information also refer to [7]

Standards

Parts of this chapter have been extracted from [9].

ISO 14443

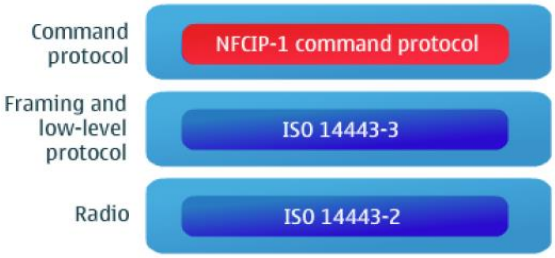
ISO 14443 is a four-part international standard originally developed for contactless chip card communication over a 13.56 MHz radio:

- ISO/IEC 14443-1:2008 Part 1: defines physical characteristics
- ISO/IEC 14443-2:2010 Part 2: defines Radio frequency power and signal interface
  - Type A uses 100% ASK with modified miller encoding in the PCD->PICC direction and OOK on a 847.5kHz subcarrier in PICC->PCD direction.
  - Type B uses 10% ASK with NRZ encoding in the PCD->PICC direction and BPSK on a 847.5kHz subcarrier in PICC->PCD direction.
- ISO/IEC 14443-3:2011 Part 3: defines initialization and anticollision
- ISO/IEC 14443-4:2008 Part 4: defines transmission protocol
  - This protocol is often also referred-to as "T=CL". This is a name derived from the commonly-used contact based smart card protocols T=0 and T=1. "CL" means "contact less".

ISO18092 or NFCIP-1

Peer-to-peer communication between two NFC devices is made possible by mechanisms defined in the Near Field Communication — Interface and Protocol Specification, NFCIP-1. This key NFC specification is also known as ISO 18092 and ECMA-340.

The protocol stack in NFCIP-1 is based on ISO 14443. The main difference is a new command protocol, which replaces the topmost part of the stack.
NFCIP-1 includes two communication modes that allow an NFC device to communicate with other NFC devices in a peer-to-peer manner, as well as with NFCIP-1 based NFC tags.



ISO 21481 or NFCIP-2

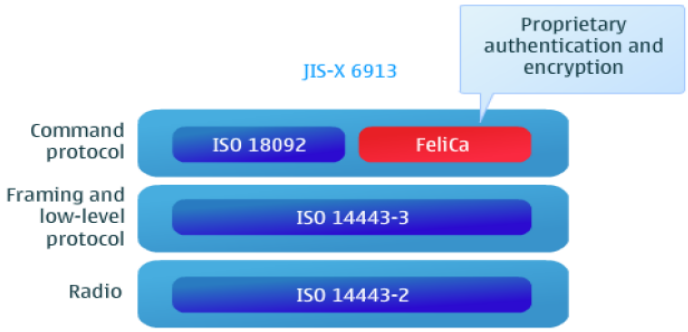
This international standard defines how an NFC object shall be able to emulate an ISO 14443 PICC (and maybe an ISO 15693 VICC).

MIFARE

MIFARE refers to an NFC tag type developed by NXP Semiconductors. MIFARE tags are widely used as memory cards in transportation applications. ISO 14443 defines a protocol stack from the radio layer up to a command protocol.

FeliCa

FeliCa is a proprietary NFC tag technology developed by Sony, and it is widely used in proprietary payment and transportation applications in the Asian markets. FeliCa tags have also been integrated with select mobile phone models in the Mobile FeliCa system. FeliCa tags are standardized as a Japanese industry standard. The tags are based on the passive mode of ISO 18092, with added authentication and encryption capabilities.



ISO 7816-1 and ISO 7816-2

This international standard defines the hardware characteristics of the ICC. The standard smartcard format (86x54mm) is called ID-1. A smaller form-factor is used for SIM cards (used in mobile phone) or SAM (secure authentication module, used for payment or transport applications) and is called ID-000.

ISO 7816-3

This international standard defines two communication protocols for ICCs: T=0 and T=1. A compliant reader must support both of them.

ISO 7816-4

This international standard defines both a communication scheme and a command set. The communication scheme is made of APDUs. The command set assumes that the card is structured the same way as a computer disk drive: directories and files could be selected (SELECT instruction) and accessed for reading or writing (READ BINARY, UPDATE BINARY instructions).

NFC Forum Transmission protocols

NFC Forum released (to cover parts not defined in the previous protocols) other standards essentially concerning NDEF (NFC data exchange format) and RTD (record types for various purposes).

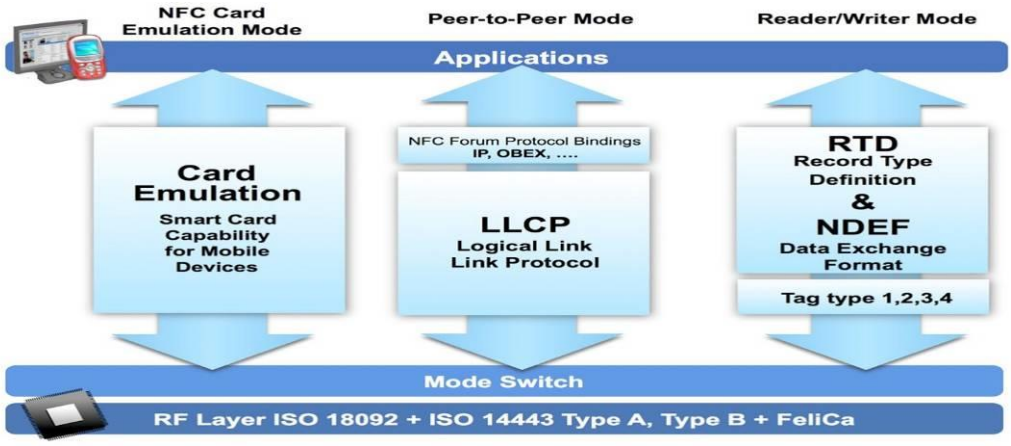
Structurally, NFC Forum specifications are based on existing and recognized standards like ISO/IEC 18092 and ISO/IEC 14443-2, 3, 4, as well as JIS X6319-4.

The NFC Forum specifications describe the parts of those standards that are relevant for NFC Forum devices.

The NFC Forum specifications cover at lower-level the digital protocols, specifically the Tag Operation specifications for the different tag types, the NFC Digital Protocol Specification, and the NFC Activity Specification.

At the physical layer it describes the NFC RF Analogue Technical Specification and at the upper-level describes the digital protocols (for example “NFC Logical Link Control Protocol (LLCP) Technical Specification" and "NFC Simple NDEF Exchange Protocol (SNPE) Technical Specification").

The illustration below describes the different components of the technical architecture of NFC in more detail.



The NFC Forum has issued 16 specifications to date:

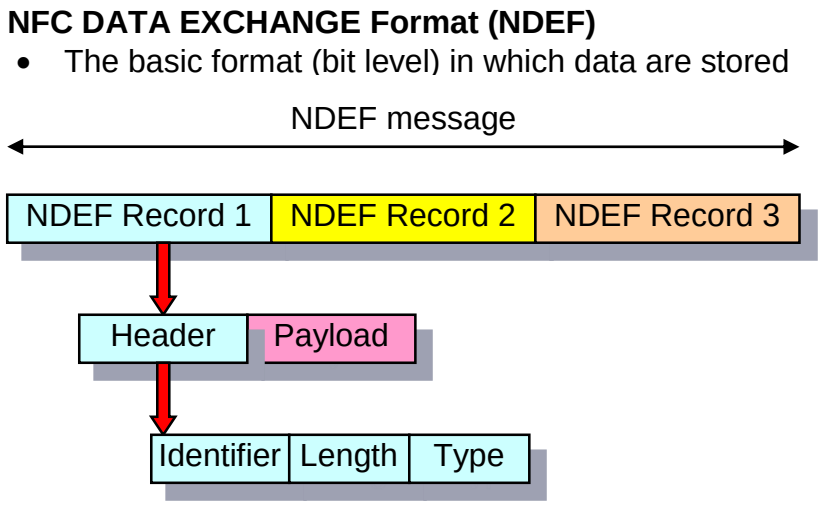
- NFC Data Exchange Format (**NDEF**) defines a common data format between NFC-compliant devices and tags
- Record Type Definition (**RTD**) specifies rules for building standard record types
- Five specific RTDs (Text, URI, Smart Poster, Generic Control, and Signature) are used to build standard record types
- Connection Handover defines how to establish a connection using other wireless communication technologies
- Operations Specifications for Four Tag Types (1/2/3/4) enable core interoperability between tags and NFC devices

- Digital Protocol addresses the digital protocol for NFC-enabled device communication, providing an implementation specification on top of the ISO/IEC 18092 and ISO/IEC 14443 standards
- NFC Activity Technical Specification explains how to set up the communication protocol with another NFC device or NFC tag
- Simple NDEF Exchange Protocol (**SNEP**) supports peer-to-peer communication between two NFC-enabled devices, which is essential for any NFC applications that involve bi-directional communications
- Logical Link Control Protocol **(LLCP**) defines a protocol to support peer-to-peer communication between two NFC-enabled devices

For more information see [10] and [11]

NFC Data Exchange Format (NDEF)

NDEF defines a message encapsulation format to exchange information between NFC devices. The NDEF is used to encapsulate one or more application-defined payloads of arbitrary type and size into a single message construct. Each payload is described by a type, a length, and an optional identifier. Type identifiers may be URIs, MIME media types, or NFC-specific types. This latter format permits compact identification of well-known types commonly used in NFC Forum applications, or self-allocation of a name space for organizations that wish to use it for their own NFC-specific purposes.



The NDEF standard includes several **Record Type Definitions (RTDs)** that define how information like URIs should be stored, and each NDEF device, tag or message can contained multiple RTDs. Standard RTD definitions are described in "NFC Record Type Definition (RTD) Specification".
For more information about creating a NDEF Message, please refer to the URI Record Type Definition, available on NFC Forum Web site [13] [12]

MIFARE Application Directory (MAD)

The MIFARE Application Directory (MAD version 1, 2 and 3) standard proposes the introduction of common data structures for card application directory entries (The MAD indicates which sector(s) contains which NDEF record).
The MAD (not present in Mifare Ultralight card 32 byte) is software integrated on Mifare Classic (NRND - Not Recommended for New Design) and hardware integrated on DesFire cards.
MAD1 can be used in any Mifare Classic card regardless of the size of the EEPROM, although if it is used with cards larger than 1KB only the first 1KB of memory will be accessible for NDEF records. The MAD1 is stored in the Manufacturer Sector (Sector 0x00) on the Mifare Classic card.
MAD2 can only be used on Mifare Classic cards with more than 1KB of storage (Mifare Classic 4K cards, etc.). It is not compatible with cards containing only 1KB of memory. The MAD2 is stored in sectors 0x00 (the Manufacturer Sector) and 0x10.
MAD3 specifies the usage of registered application identifiers in the context of MIFARE DesFire.
MIFARE DesFire cards features a flexible file system which organizes user data in applications which hold files. Applications are identified with a 3 byte application identifier (AID). AIDs have to be unique per card and are defined at application creation time. A dedicated list of currently installed application does not have to be maintained by the card issuer, as the MIFARE DesFire IC maintains this list automatically. To collect a list of applications on a card, the MIFARE DesFire command GetApplicationIDs is used. This command returns a list holding all MIFARE DesFire AIDs present on the card.

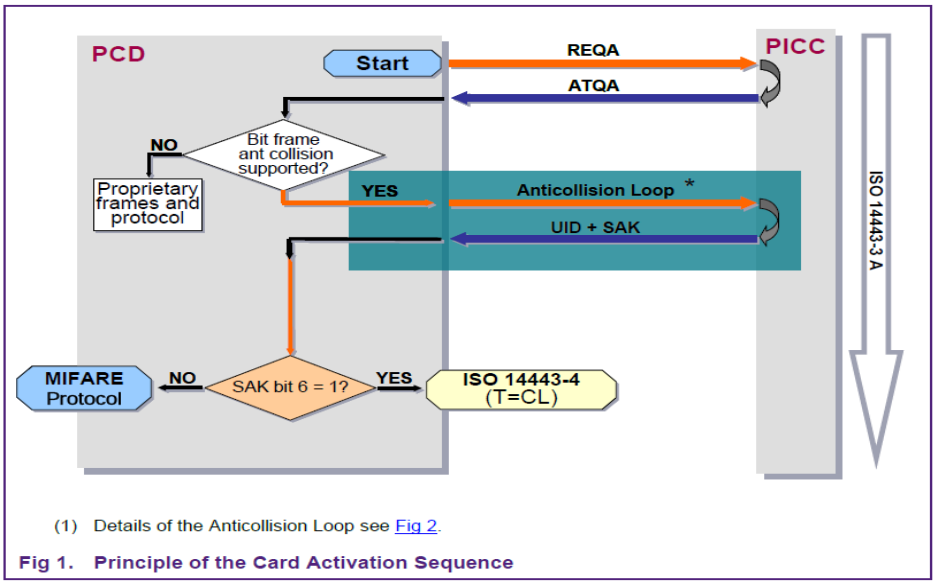
Other important Documents

MIFARE Type Identification Procedure (AN10833)

This Application note describes how to differentiate between the members of the MIFARE card IC family. ISO/IEC 14443-3 describes the initialization and anti-collision procedure, and ISO/IEC 14443-4 describes the protocol activation procedure. This document shows how to use these procedures to deliver the chip type information for all MIFARE ICs. The anti-collision procedure is mandatory for ISO/IEC 14443A compliant PICCs.

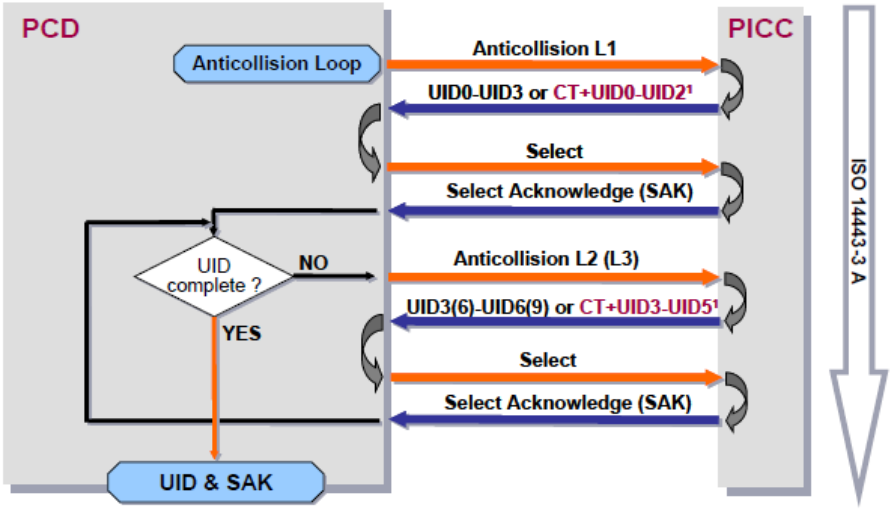
The PCD (Proximity Coupling Device - “Contactless Reader”) typically polls for PICCs (Proximity Integrated Circuit -“Contactless Card”) in the field. This is done with the REQA (Request Command, Type A).
When a PICC is within the operating range of the PCD and receives the REQA (Request Command, Type A), any MIFARE PICC returns the ATQA (Answer to Request acc. to ISO/IEC 14443-4). The content of the ATQA should be ignored in a real application, even though according to the ISO/IEC 14443 it indicates that the PICC supports the Anticollision scheme.

Note: In the case two or more MIFARE PICCs are in the operating field of the PCD at the same time, the received (combined) ATQA might contain “collisions”. That means there might be no unambiguous content anyway. The complete card activation sequence is shown in the Fig 1 and Fig 2. The bit 63 in the SAK (Select Acknowledge, Type A) indicates, whether the PICC is compliant to the ISO/IEC14443-4 or not. However, it does not necessarily indicate, whether the PICC supports the MIFARE Protocol or not. For more details about selecting the different type of MIFARE cards refer to the AN “MIFARE ISO/IEC 14443 PICC Selection”.



(1) Details of the Anticollision Loop see Fig 2.

Fig 1. Principle of the Card Activation Sequence



(1) The CT (= Cascade Tag, Type A) byte indicates that the UID is not received completely yet. It indicates that another anticollision loop on the next higher cascade level is required to get the complete UID.

Fig 2. Anticollision Loop as part of the Card Activation Sequence

Note

For more details regarding the selection of one of the different types of MIFARE cards based on the SAK refer also to AN 130830 “MIFARE ISO/IEC 14443 PICC Selection”.

MIFARE ISO/IEC 14443 PICC Selection (AN10834 by NXP)

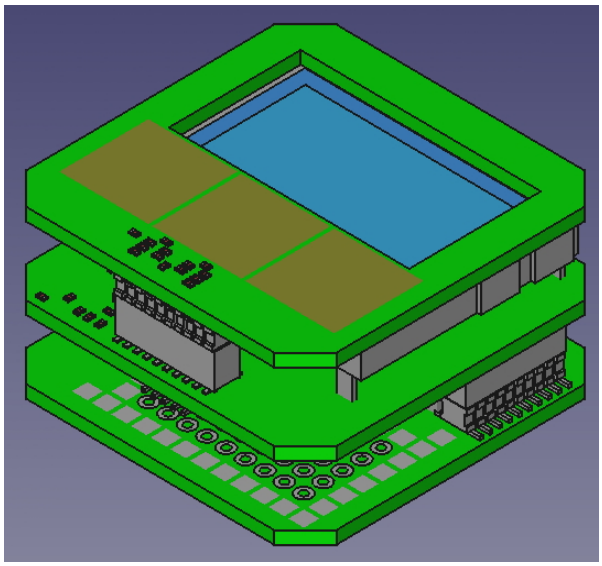
This Application Note shows the elementary communication for selecting a Contactless Smart Card according to the ISO/IEC 14443 (that describes how to select “activate” a single card), and how to use this communication to guarantee proper functionality in different applications.

Note

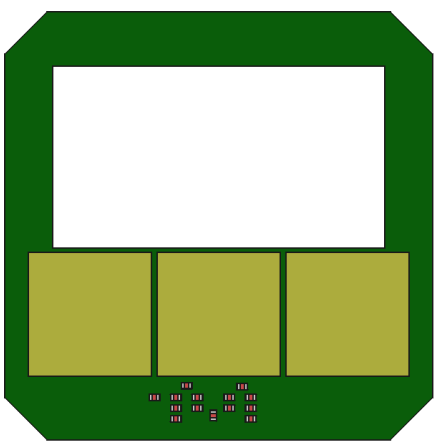
Standards are extremely important and not all standards or relevant documents are included in this file.
More information is available on Internet and on Standards’ web sites.

5 SmartTool

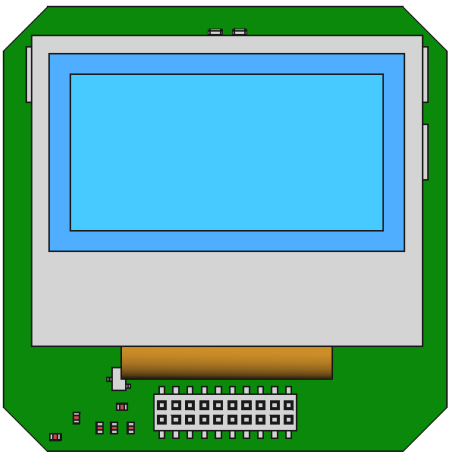
All required documentation to reproduce SmartTool hardware is included in this reference design.
SmartTool consists of three PCBs (4 layers each) layered on top of each other.



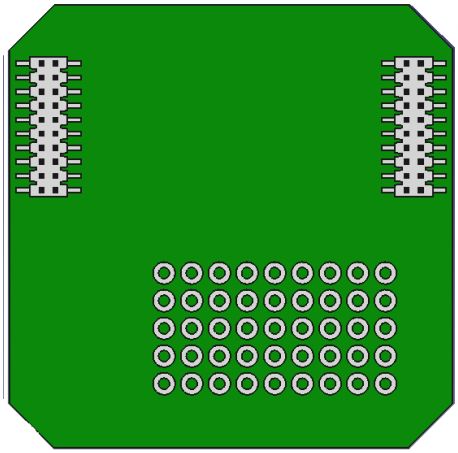
Assembled SmartTool



HMI BOARD

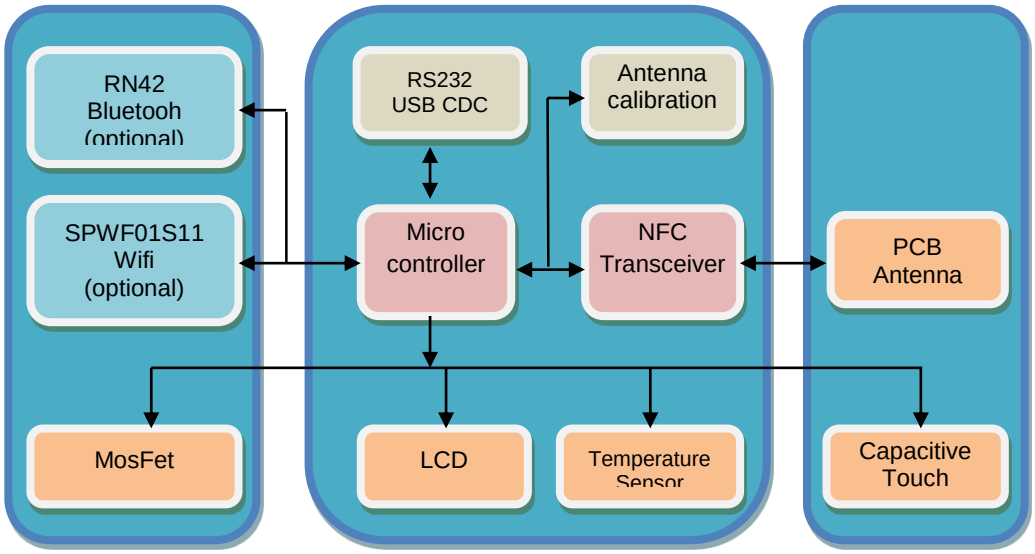


MAIN BOARD



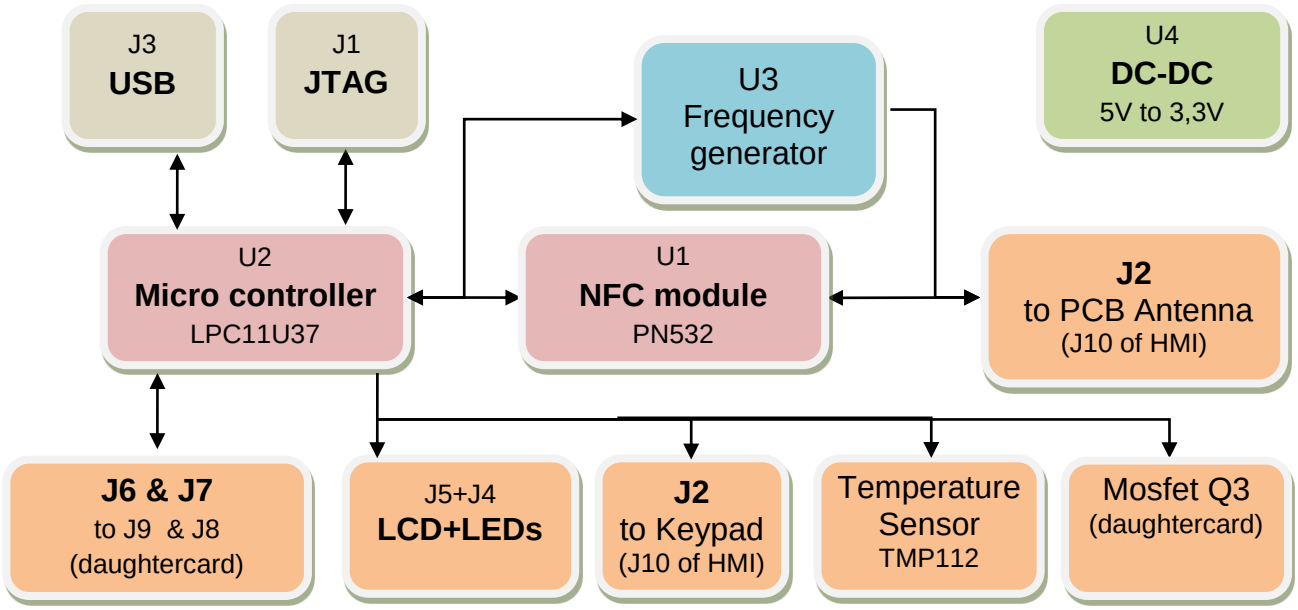
DAUGHTERCARD BOARD

Block diagram of the three boards is as follows:

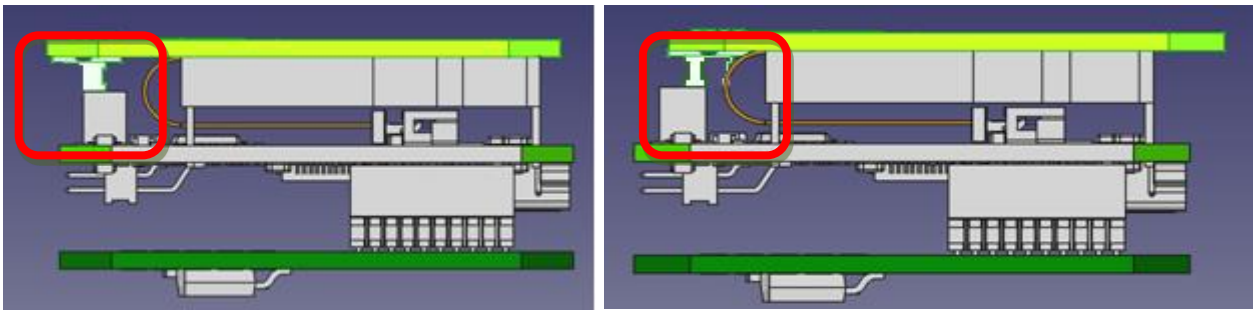


Main Board

The “Main board” includes a transceiver module for contactless communication (PN532), a microcontroller with Full Speed USB 2.0 (LPC11U37), a step down DC-DC converter (TPS62291), an ultra-low jitter clock at high-speed differential frequencies chip (SI5351A-B-GT) used for antenna calibration and an LCD.

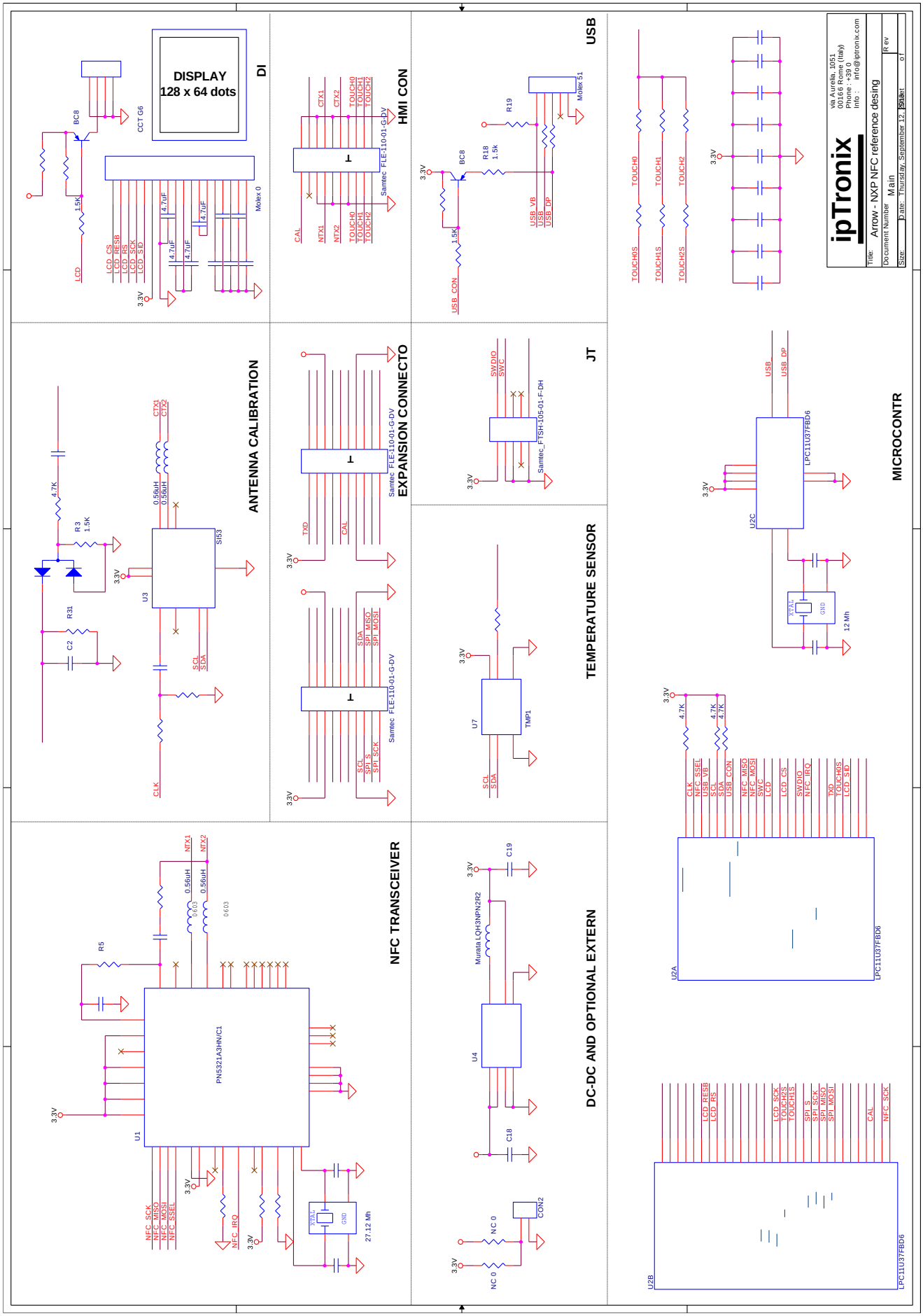


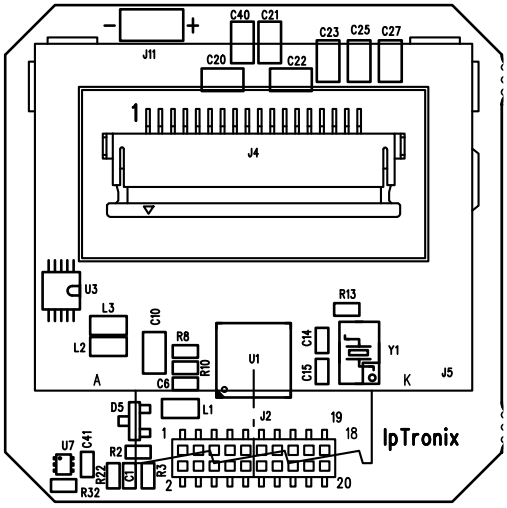
The clock generator chip (U3), connected to J2, allow antenna calibration when J10 connector of HMI board is inserted in the internal row of J2. When J10 is connected to the external row of J2, the antenna PCB is connected to PN532 and works in application mode.



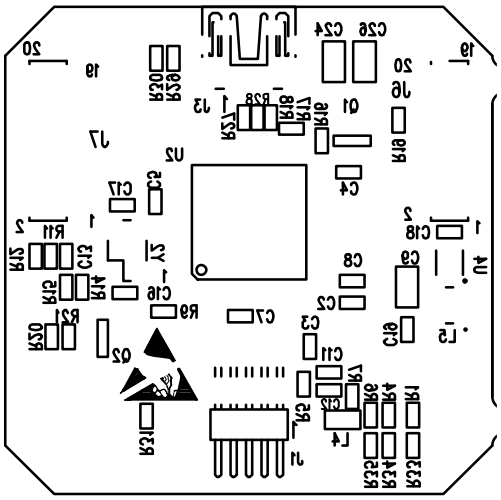
Normal Mode **Antenna Calibration Mode**

An USB connector is available to provide power supply and to implement USB device functionality. A JTAG connector is also present to allow on board debugging via LPCXpresso boards.


DISPLAY
128 x 64 dots
DI
HMI CON
USB
ANTENNA CALIBRATION
EXPANSION CONNECTO
JT
TEMPERATURE SENSOR
NFC TRANSCEIVER
DC-DC AND OPTIONAL EXTERN
MICROCONTR
ipTronix
Via Aurelia, 1051
00165 Roma (Italy)
Phone : +39 0
info : info@iptronix.com
Title: Arrow - NXP NFC reference desing
Document Number
Main
Rev
Size:
Date: Thursday, September 12,
Sheet
of



Top layer silkscreen PCB



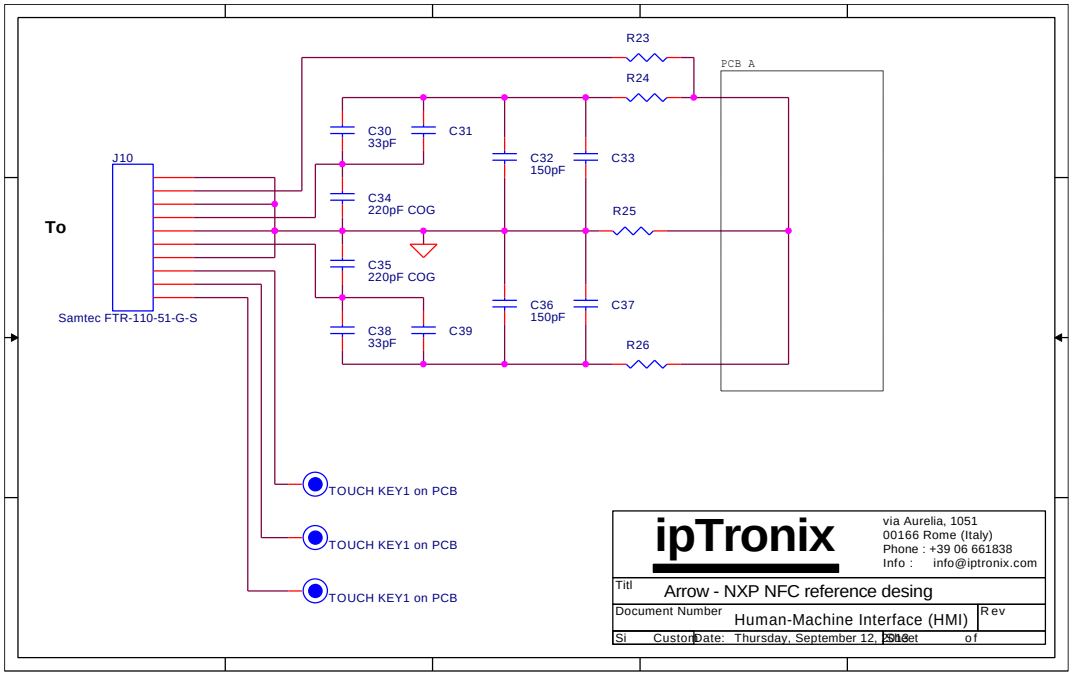
Bottom layer silkscreen PCB

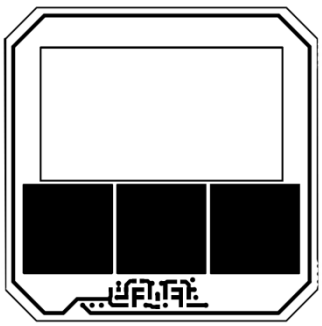
HMI Board

The “HMI board” (Human-Machine Interface board) includes three touch pads (TP8, TP9, TP10) and the PCB antenna.

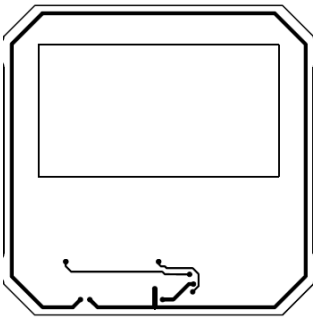
Touch keys are a simple gold plated copper pad on the top layer of the PCB.
Antenna is a 4 winds coil made with octagon shaped PCB traces running parallel on the 4 layers.

This board is connected with Main Board’s J2 via the J10 connector.

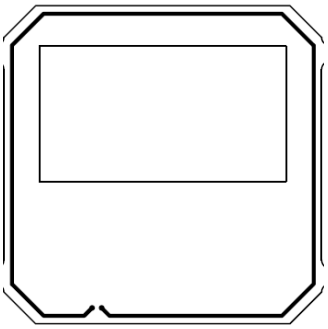




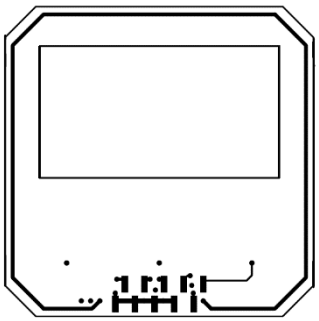
Top Layer



Inner Layer 2

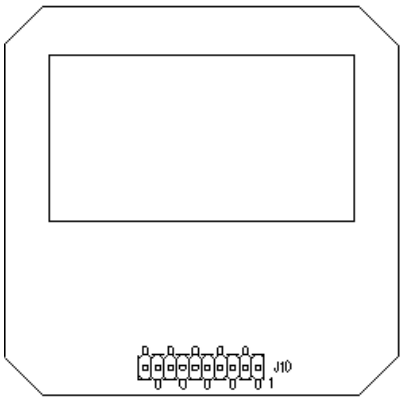


Inner Layer 3



Bottom Layer

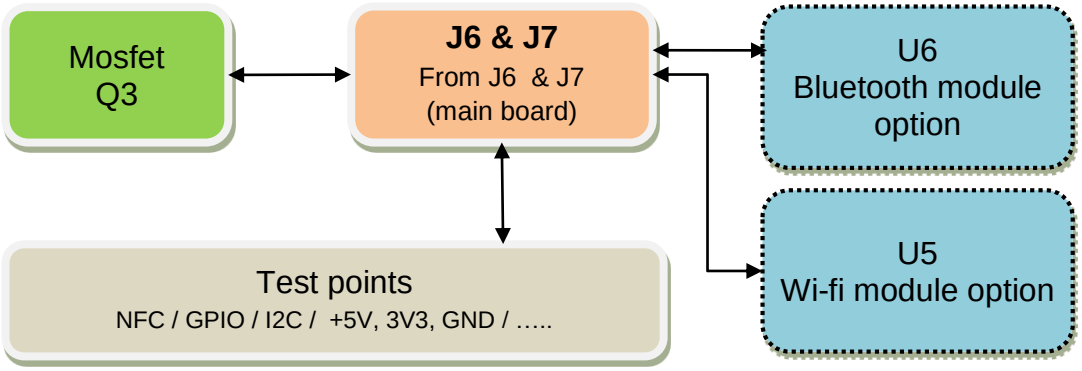
Top layer silkscreen PCB

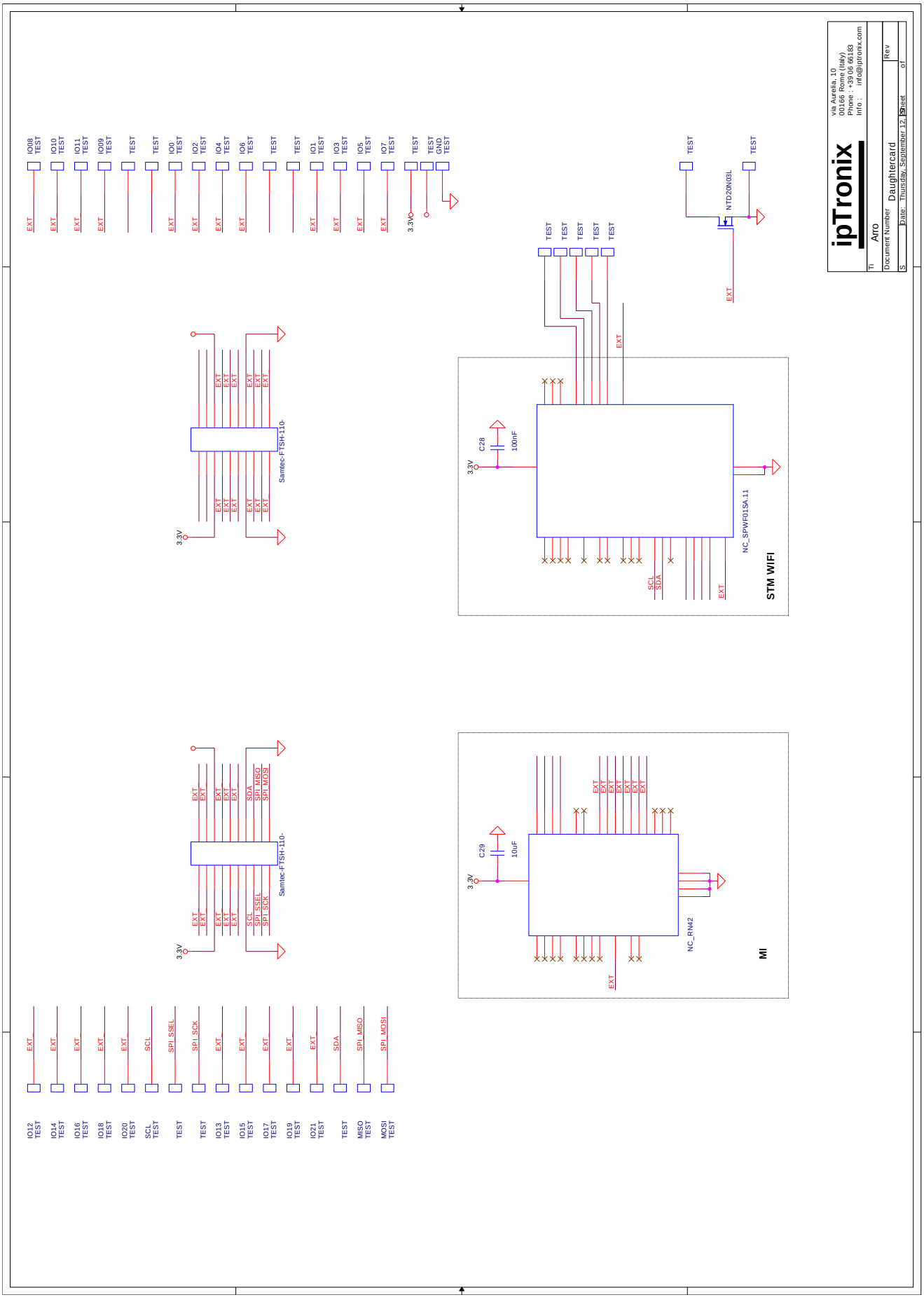


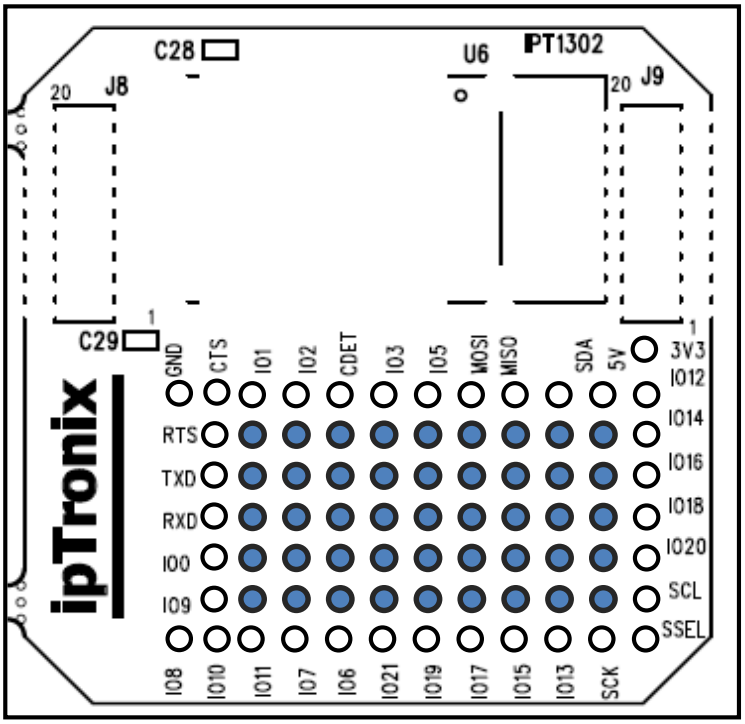
Bottom layer silkscreen PCB

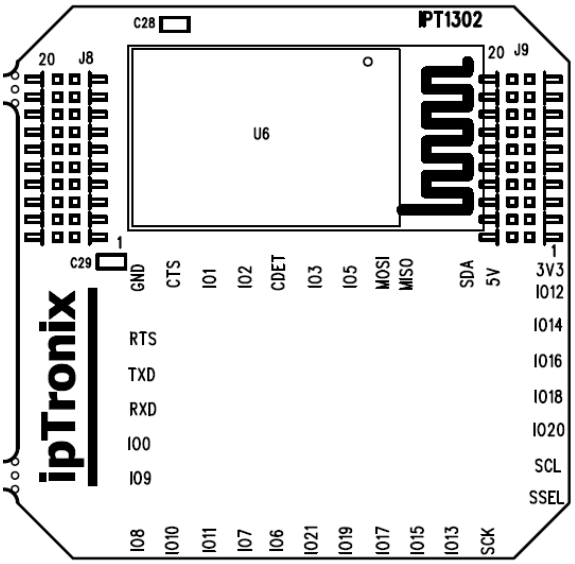
Daughtercard

DAUGHTERCARD includes a breadboarding area whose perimeter is connected to almost all microcontroller pins.
In addition in the prototyping area a power mosfet is available to drive high current DC loads as for example a relay, a valve or similar.
Optional pads for assembling a RN42 Bluetooth module from Microchip or a SPWF01SA Wi-Fi module from STMicroelectronics are provided via U6 and U5.
Note that Wi-Fi and Bluetooth modules are not officially supported on the reference software and are not mounted on the boards.

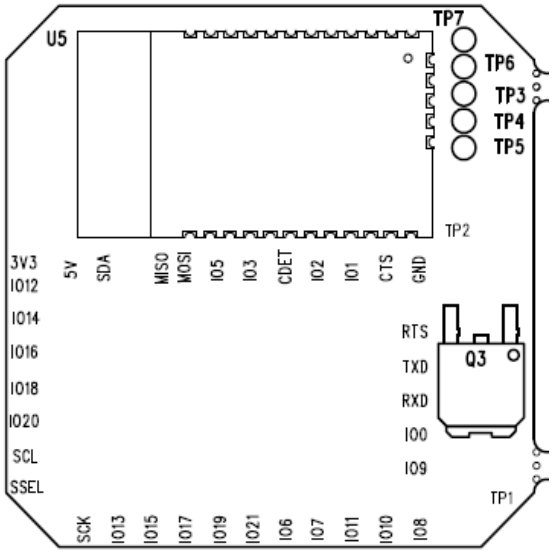



ipTronix
via Aurelia, 10
00166 Rome (Italy)
Phone : +39 06 87 67 83
Info : info@ipronix.com
Ti Arro
Document Number Daughtercard
Rev
S Date: Thursday, September 12, 2013 Sheet of
STM WIFI
MI
NC_SPWF01SA.11
NC_RN42
NTD20N03L
Samtec-FTSH-110-
C28
100nF
C29
10uF
3.3V
EXT
TEST
SCL
SDA
SPI_MISO
SPI_MOSI
SPI_SSEL
SPI_SCK





Top layer silkscreen PCB



Bottom layer silkscreen PCB

SmartTool Power supply

SmartTool is powered via the 5V coming from the USB connector available on the MAIN board.

No additional power supply is required to operate SmartTool

USB mini B connector (type A) of IPT1302

- Molex P/N: 51387-0530

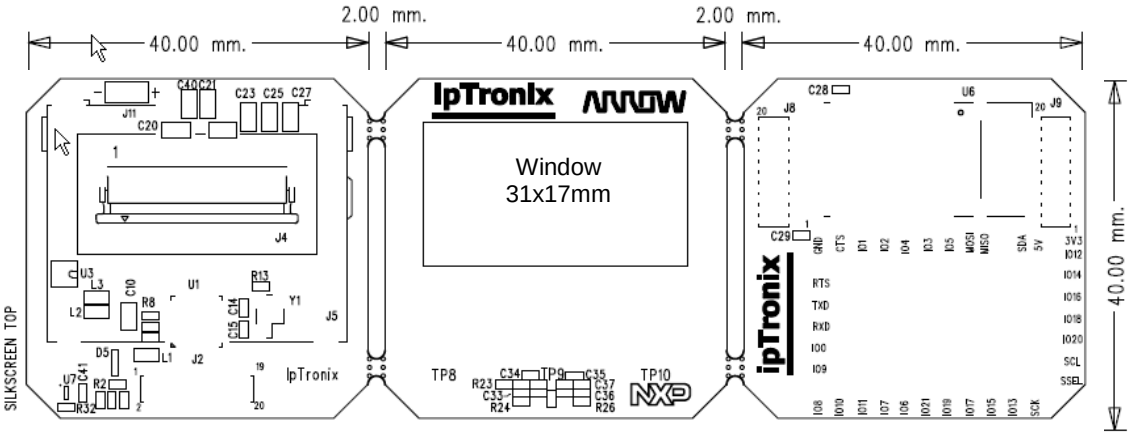
USB cable required to connect SmartTool to PC (USB A plug):

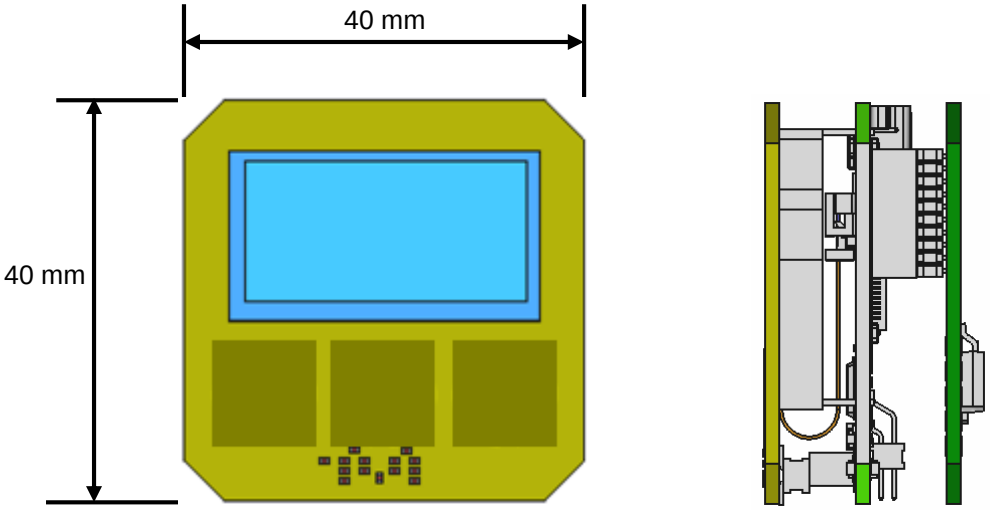
- Molex P/N : 88732-8600 or equivalent.

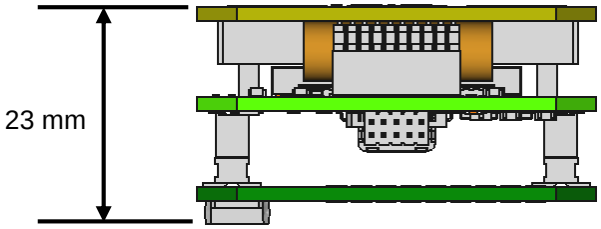
Mechanical specifications:

PCB thickness is 1,6mm, the copper thickness is 35um.

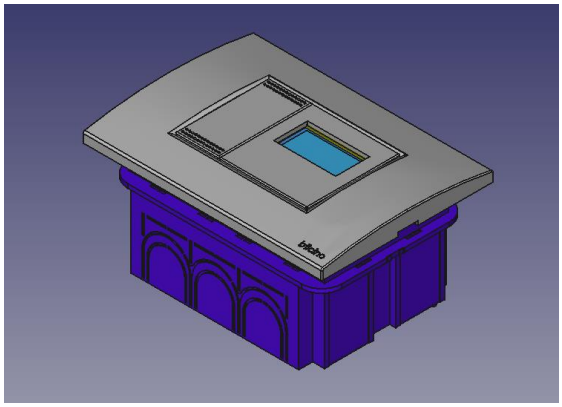
The maximum dimensions of PCBs are:

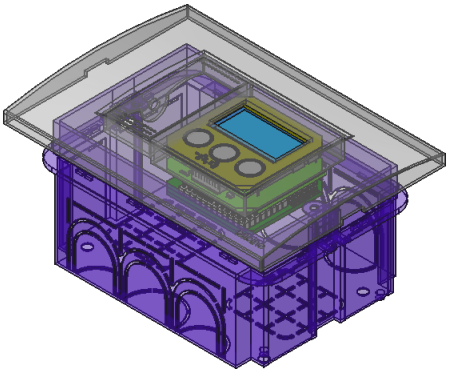


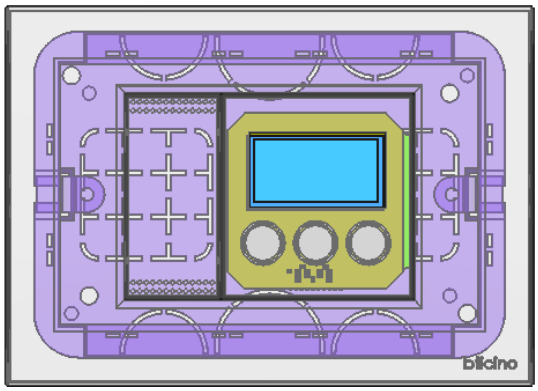


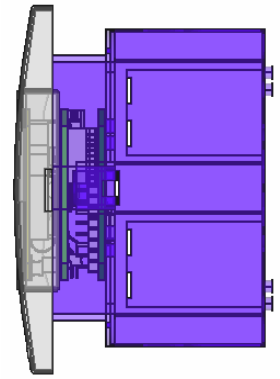


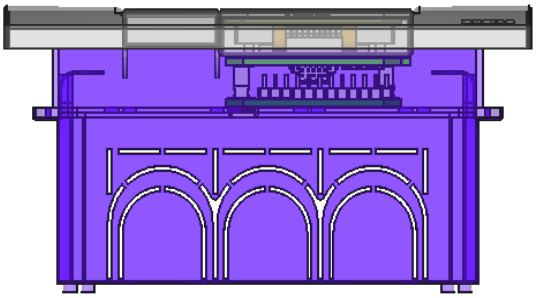
The shape and size of assembled SmartTool allows easy insertion into two modules of a wall enclosure such as 503 series (example Bticino p/n:503E or Vimar p/n:V71303)











Example of installation:

6 Components used in SmartTool

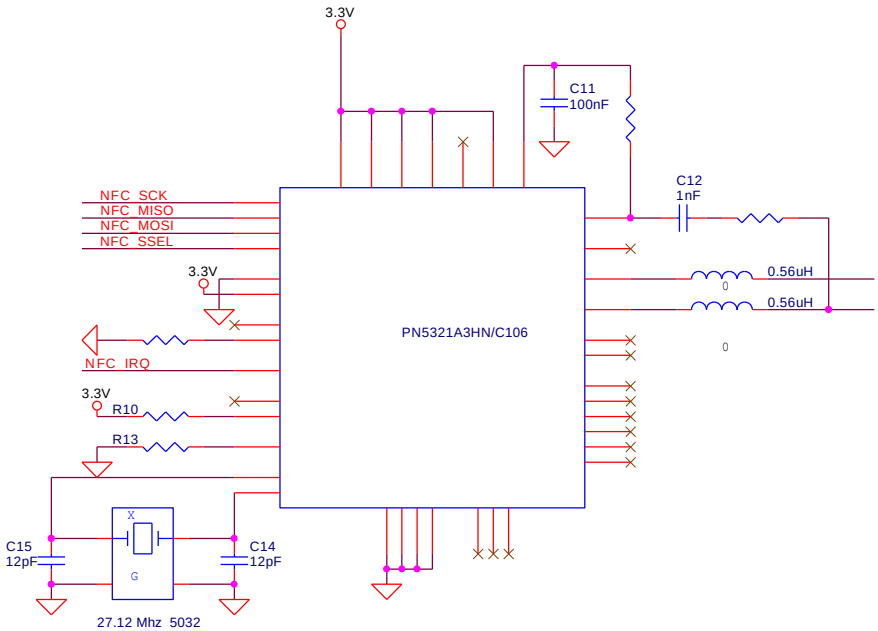
SmartTool uses the following components

PN5321A3HN/C106 (NXP)

Main board hosts a PN5321A3HN/C106; from here on referred to as PN532.
PN532 is a highly integrated transceiver module for contactless communication at 13.56 MHz based on the 80C51 microcontroller core.
It supports 6 different operating modes:

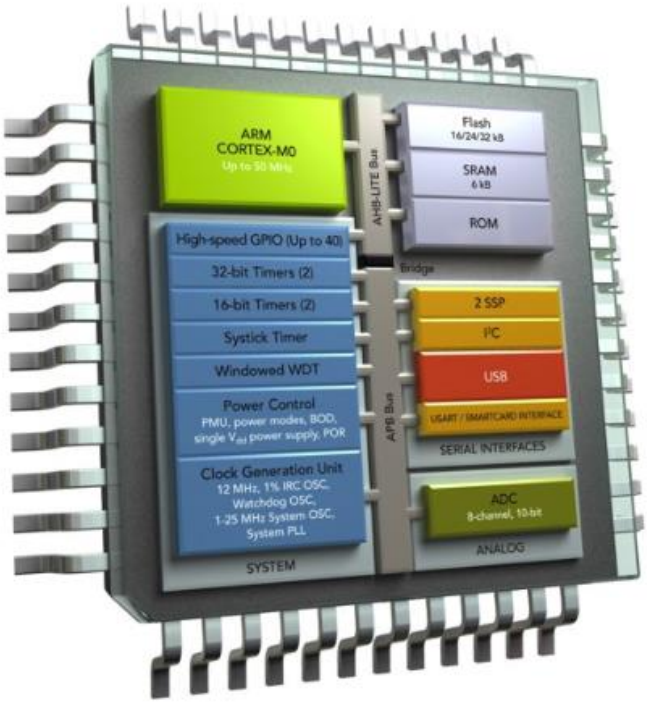
- ISO/IEC 14443A/MIFARE Reader/Writer
- FeliCa Reader/Writer
- ISO/IEC 14443B Reader/Writer
- ISO/IEC 14443A/MIFARE Card MIFARE Classic 1K or MIFARE Classic 4K card emulation mode
- FeliCa Card emulation
- ISO/IEC 18092, ECMA 340 Peer-to-Peer

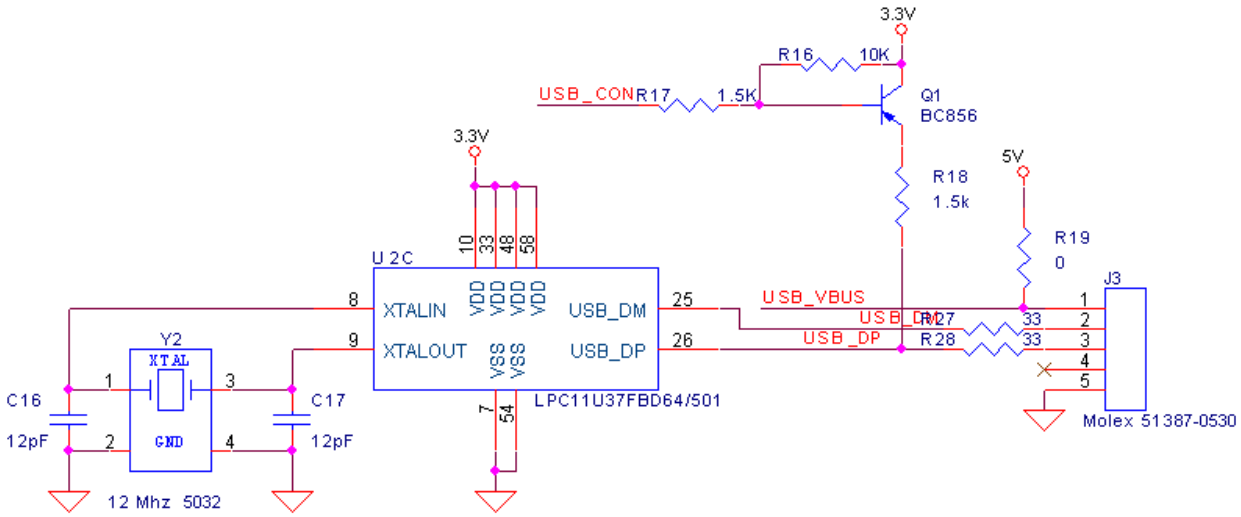
Compliant to ECMA 340 and ISO/IEC 18092 NFCIP-1 Passive and Active communication modes, the PN532 offers the possibility to communicate to another NFCIP-1 compliant device, at transfer speeds up to 424 kbit/s.
The PN532 transceiver can be connected to an external antenna for Reader/Writer or Card/PICC modes, without any additional active component.

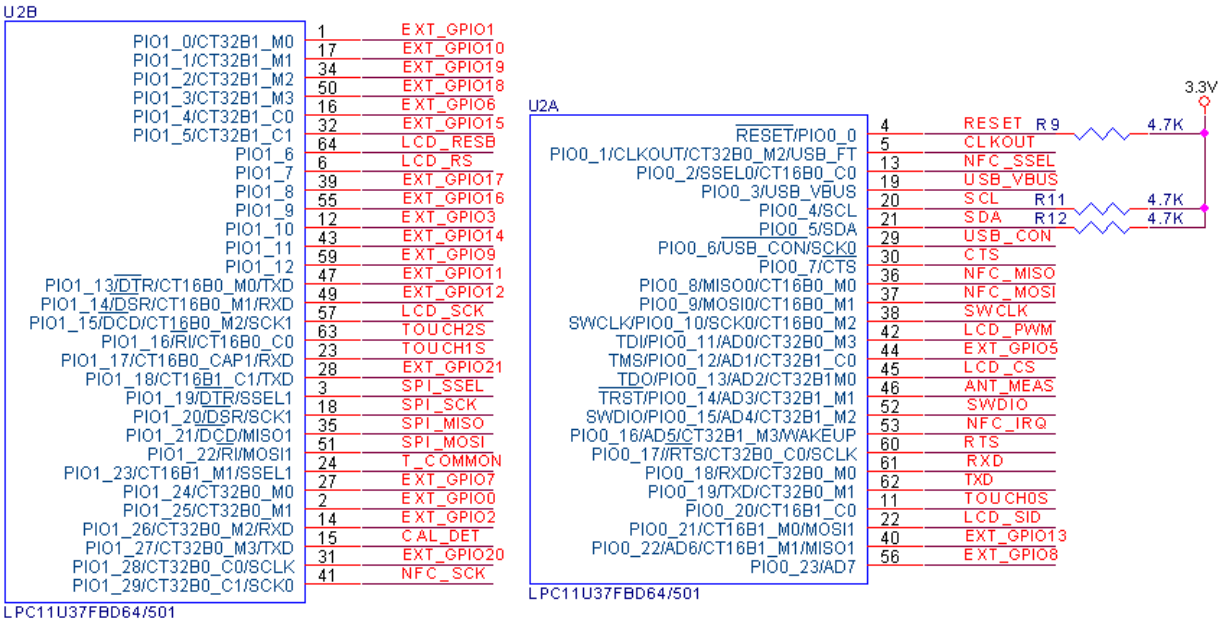


LPC11U37FBD64/501 (NXP)

Main board's microcontroller is a LPC11U37FBD64, a Cortex-M0 based, low-cost 32-bit MCU, designed for 8/16-bit microcontroller applications, low power, simple instruction set and memory addressing together with reduced code size compared to existing 8/16-bit architectures. The LPC11U37FBD64 operates at CPU frequencies of up to 50 MHz. Equipped with a highly flexible and configurable Full Speed USB 2.0 device controller.







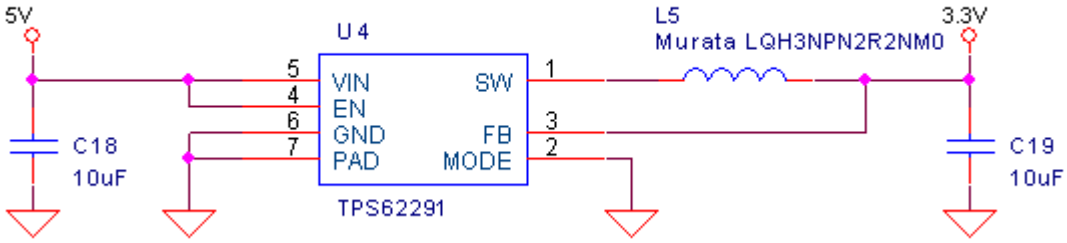
TPS62291 (Texas Instruments)

TPS62291 is a highly efficient synchronous step down dc-dc converter optimized for battery powered portable applications. It provides up to 1000-mA output current from a single Li-Ion cell.

With an input voltage range of 2.3 V to 6 V, the device supports batteries with extended voltage range and is ideal to power portable applications like mobile phones and other portable equipment.

The Power Save Mode is optimized for low output voltage ripple.

The TPS62291 allows the use of small inductors and capacitors to achieve a small solution size and no external components are needed (excluded coil) in 5V input/3.3V output configuration.

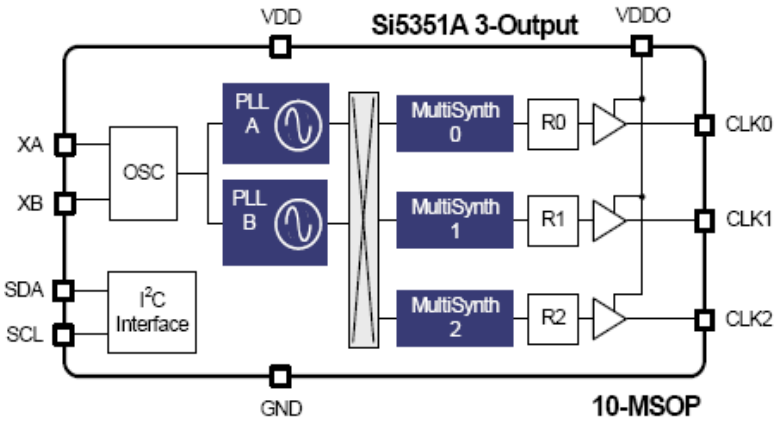


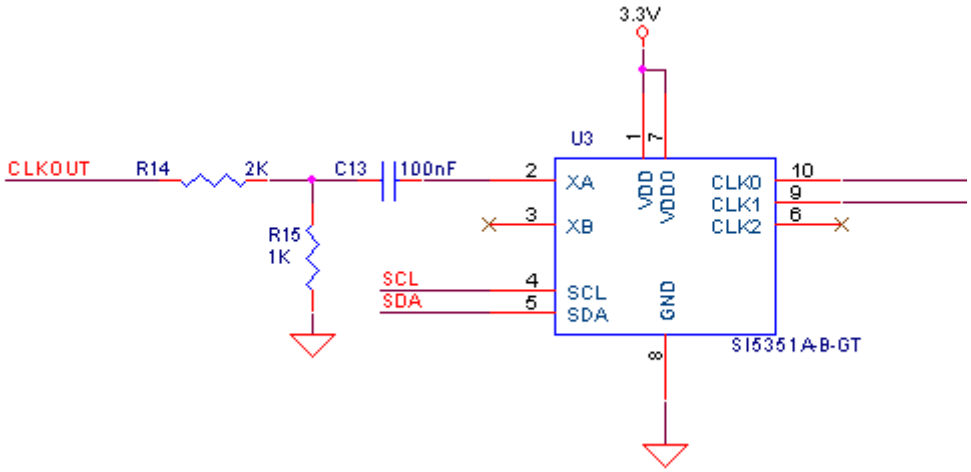
SI5351A-B-GT (Silicon Laboratories)

Si5351 is a highly flexible clock generator configurable through its I2C interface.

The SI5351A-B-GT provide an ultra-low jitter clock at high-speed differential frequencies and use one fixed crystal to provide a wide range of output frequencies. This IC based approach allows the crystal resonator to provide exceptional frequency stability and reliability. In addition, DSPLL clock synthesis provides superior supply noise rejection, simplifying the task of generating low jitter clocks in noisy environments typically found in communication systems.

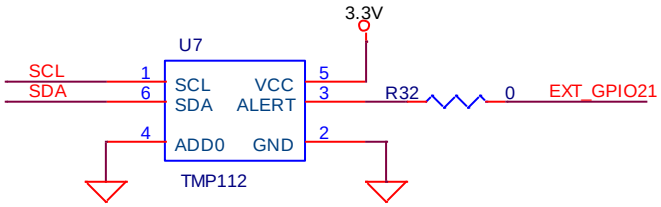
The Si5351 can be driven with a clock signal through the XA input pin to replacing an external Crystal.





Temperature Sensor (Texas Instruments)

TMP112 is a two-wire serial output temperature sensor with a resolution of 0.0625°C.
The TMP112 features both SMBus and two-wire interface compatibility, and allows up to four devices on one bus.
Note that due to main board self-heating, it is possible that measured temperature will be higher than ambient temperature especially if components such as the microcontroller are in continuous operation.

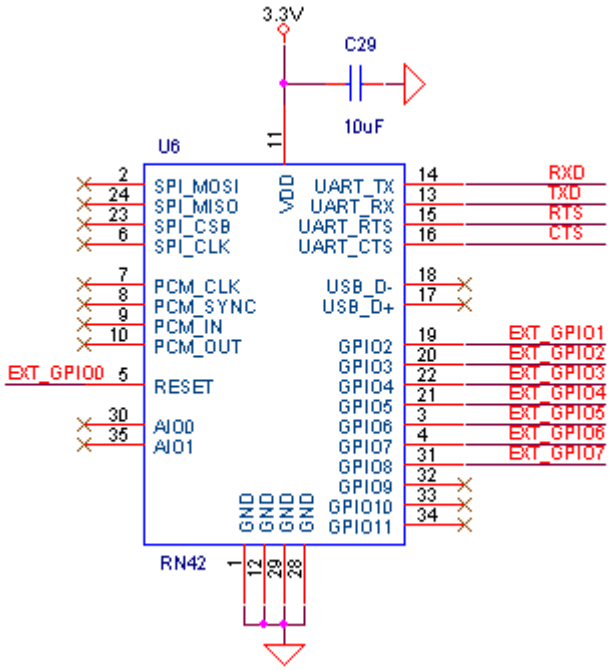


Optional Components

Daughtercard contains footprints for wireless modules that are not mounted and for which software is not provided in this reference design.

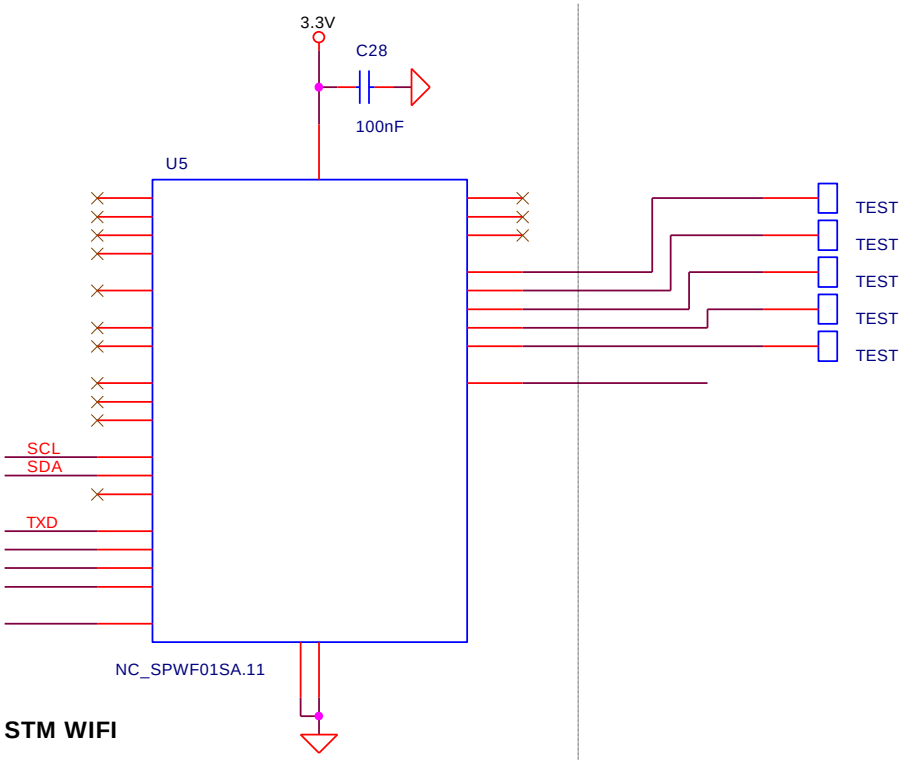
RN42 (Microchip Technology)

RN42 is a small form factor, low power, class 2 Bluetooth radio, which is fully certified and supports multiple interface protocols.
With its high-performance, on-chip antenna and support for Bluetooth EDR, the RN42 delivers up to a 3 Mbps data rate for distances up to 20 meters.



SPWF01SA.11 (STMicroelectronics)

The SPWF01SA.11 is a standalone WI-FI module 802.11 b/g/n web content solution that provides the full TCP/IP stack enabling end products to leverage AT Commands for wireless internet connectivity. Configured around a single-chip 802.11 transceiver, STM32 32-bit microcontroller with extensive GPIO suite, 8MBFlash, and 64KB RAM, this modules enables easy integration of wireless web access. The module incorporates timing clocks and voltage regulators.



7 Tools

The main tools used in this reference design are listed below:

LPCXpresso

LPCXpresso's IDE [3] is a highly-integrated software development environment for NXP's LPC microcontrollers, which includes all the tools necessary to develop high-quality software solutions in a timely and cost effective fashion.
The platform is comprised of a simplified Eclipse-based IDE and low-cost target boards which include an attached JTAG debugger

The LPCXpresso IDE can build an executable of any size with full code optimization, and it supports a download limit of 256KB after free registration on :www.nxp.com/lpcxpresso

LPCXpresso software can be downloadedfrom the URL: http://www.lpcware.com/lpcxpresso/download
(Windows version: LPCXpresso_6.1.0_164.exe).
Linux and Mac OS x versions are also available.

After installation, create your free account on site:
http://www.lpcware.com/user/register

With your account log in to http://www.lpcware.com/lpcxpresso/activate, and insert serial number of LPCXpresso program to create license key.

Documentation is available to:
http://www.nxp.com/documents/other/LPCXpresso_Getting_Started_Guide.pdf

LPC-Link 2

LPC-Link 2 is a stand-alone debug adapter board that can be used with LPCXpresso IDE. This board includes a standard 10-pin JTAG/SWD connector that can be connecting to J1 connector of “Main board” of IPT1302 demo board.

This board can be order to NXP by order code: OM13054.
http://www.nxp.com/demoboard/OM13054.html

As an alternative any other LPCXpresso board can be used.

http://www.nxp.com/documents/other/LPCXpresso_Getting_Started_Guide.pdf

Note

JTAG and USB cables need to be ordered separately for LPC-Link while are included in LPC-Link2.
Note also that for mechanical reasons the JTAG connector can't be inserted directly on the SmartTool board in the correct direction unless the connector key has been shaved off

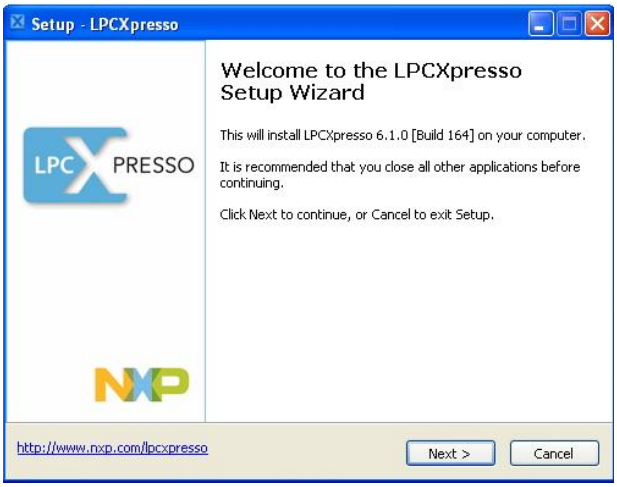
JTAG cable sample P/N is: Samtec P/N: FFSD-05-D-06.00-01-N or equivalent. (Ribbon cable, IDC, pitch connector: 1,27mm , pitch cable 0,635mm, 10 way)

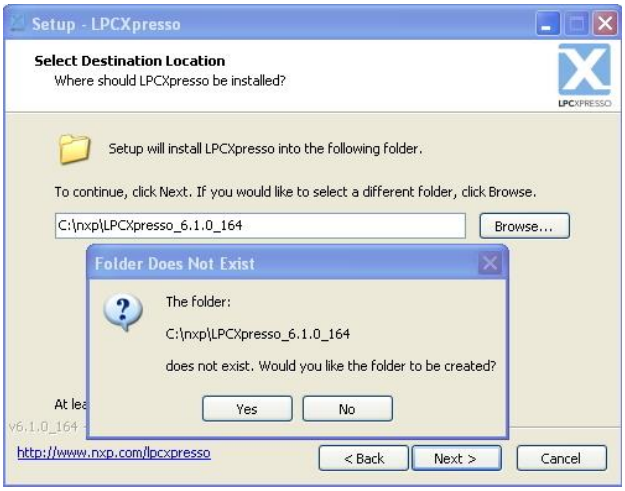
USB cable sample P/N is: Molex P/N: 88732-8600 or equivalent. (USB A plug to USB mini B plug)

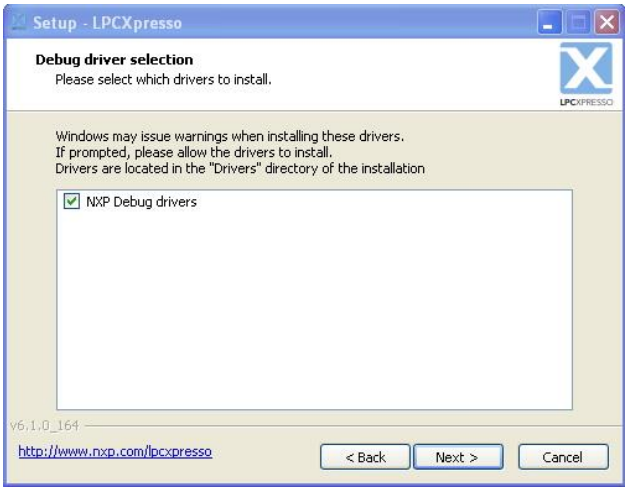
8
Software tool installation

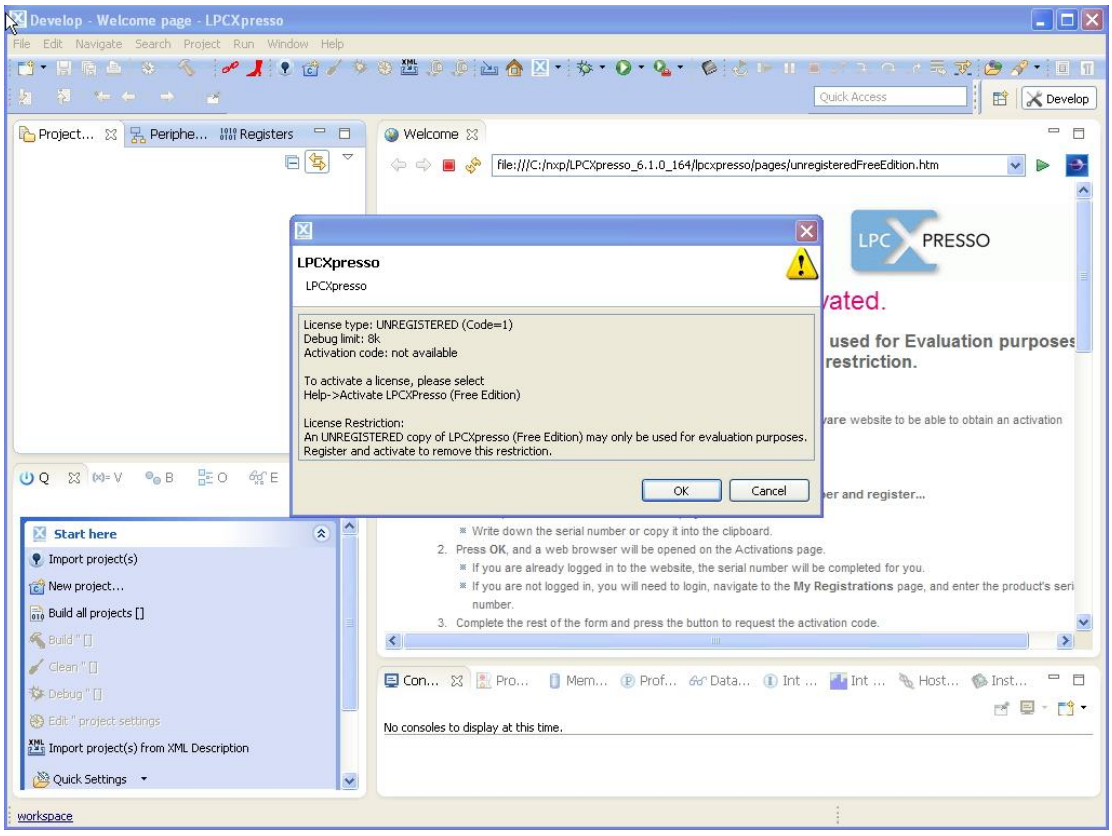
LPCXpresso installation

After downloading, install LPCXpresso (do default standard installation answering all the questions ok).

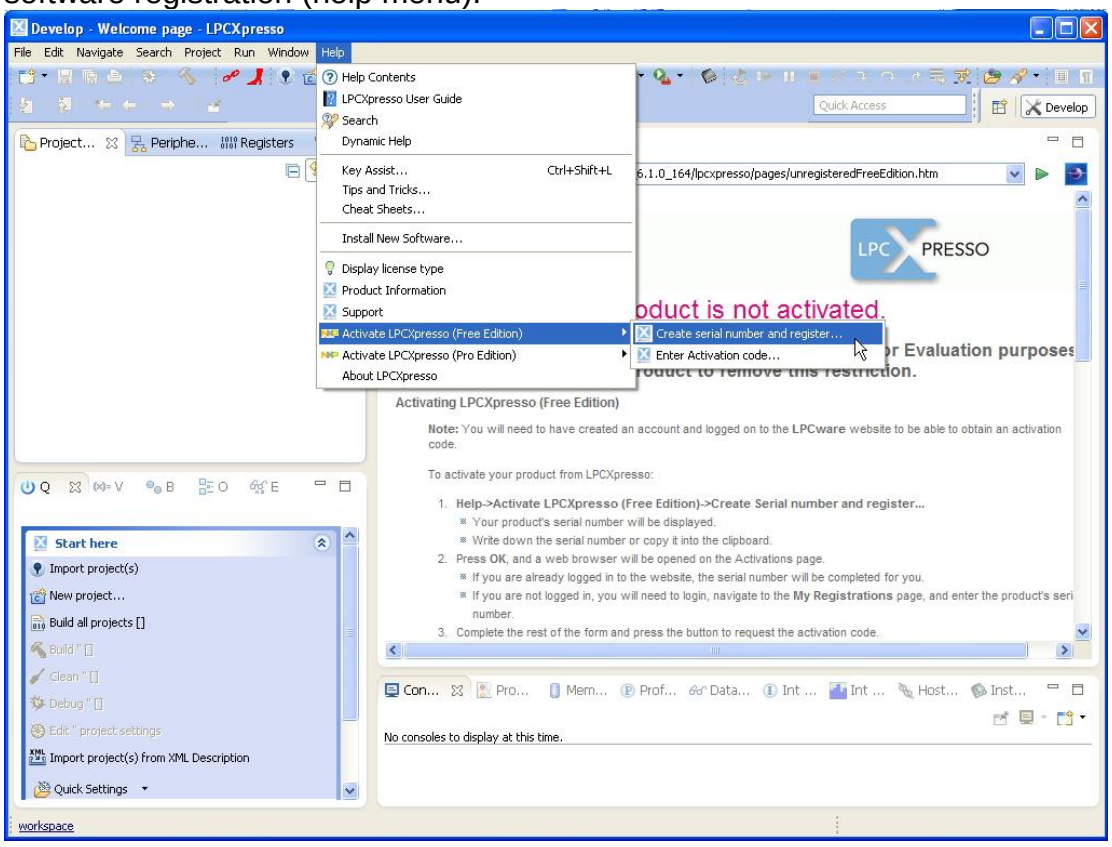






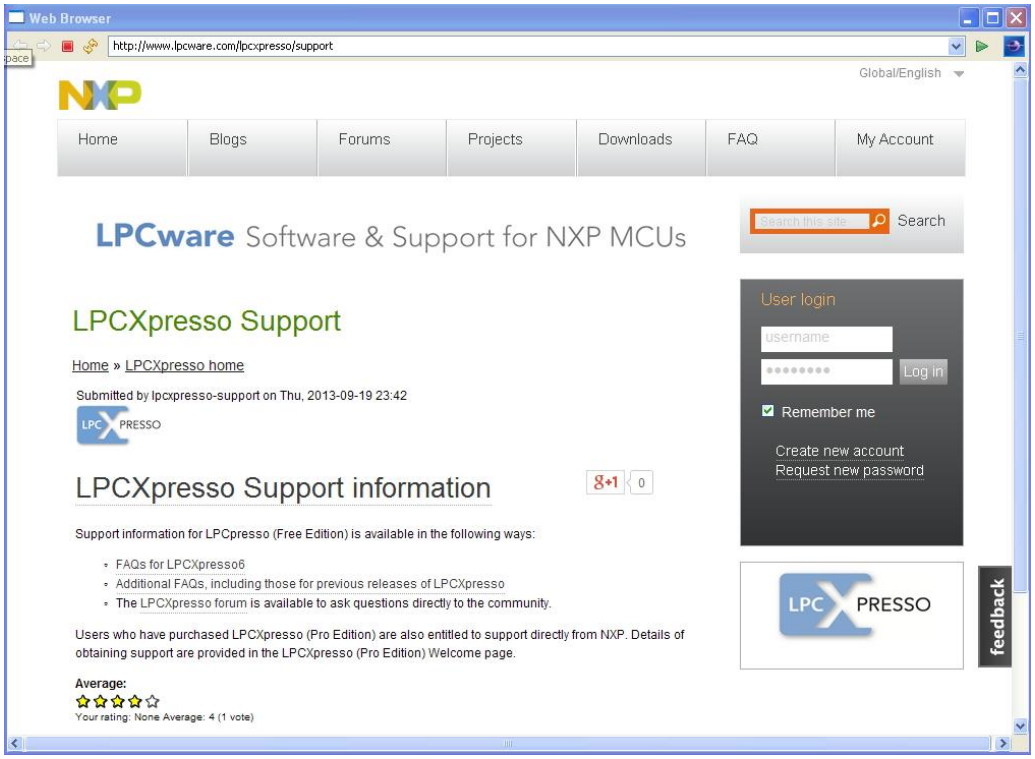


After successful installation, open LPCxpresso and proceed with free software registration (help menu).

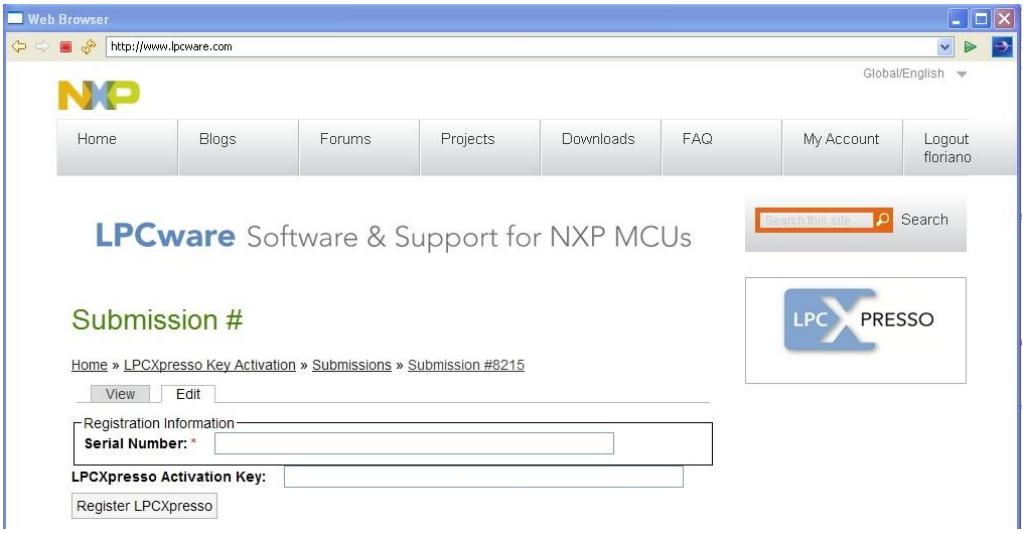


Copy serial number

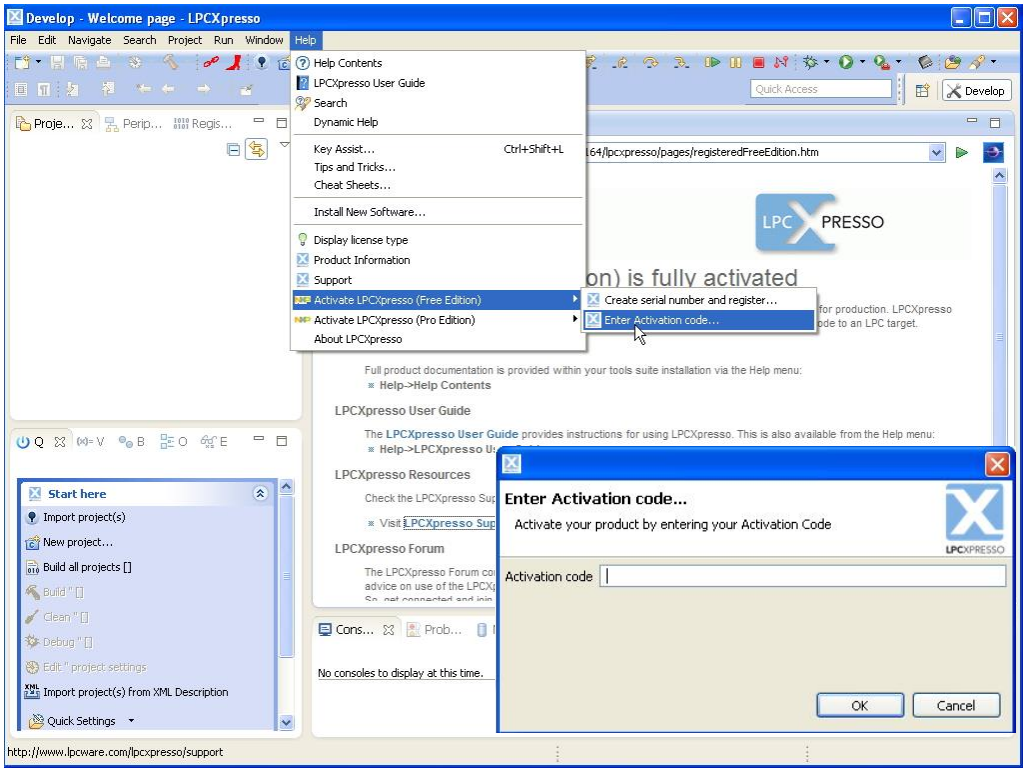
Open http://www.lpcware.com/lpcxpresso/activate url ,

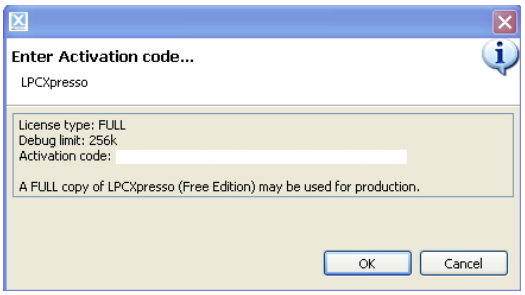


Insert serial number, press Register LPCXpresso



copy the LPCXpresso Activation Key on software window



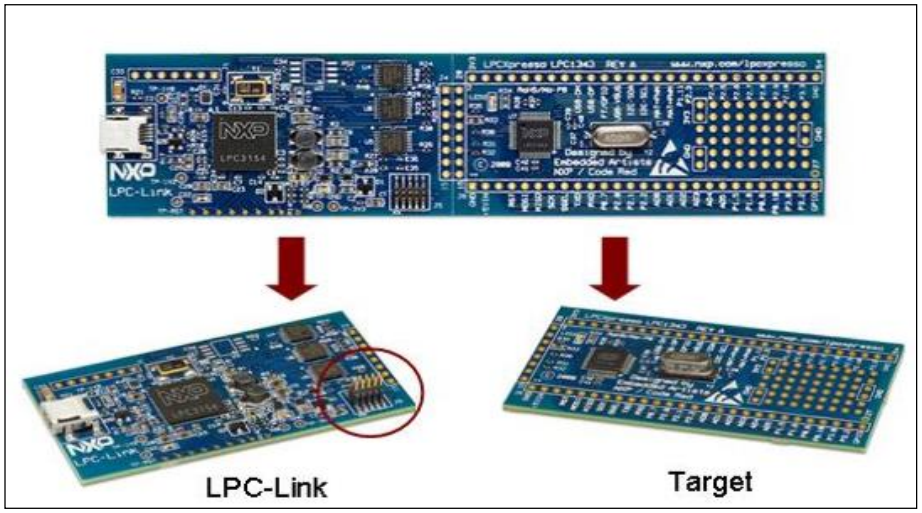


For any question read “LPCXpressoGettingStarted.pdf” file or go to www.nxp.com/lpcxpresso.

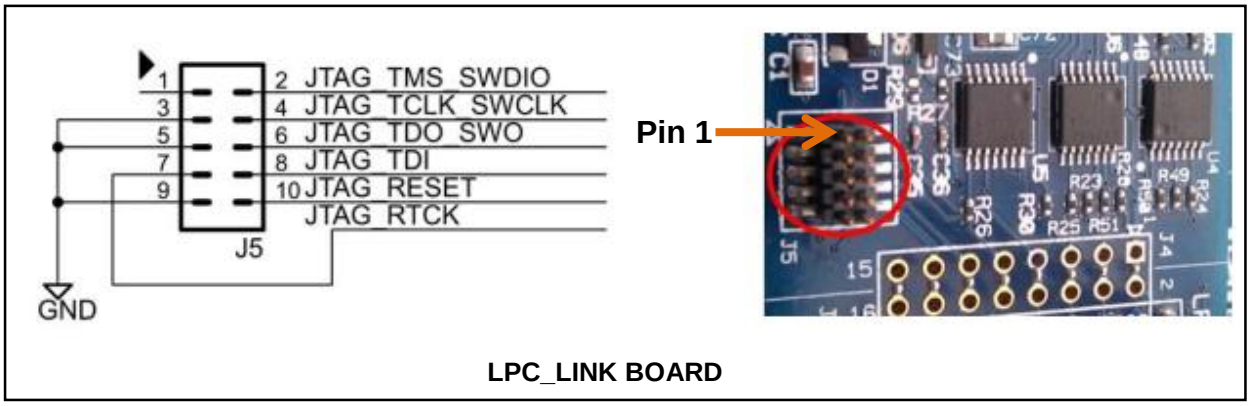
Documentation is available at:
http://www.nxp.com/documents/other/LPCXpresso_Getting_Started_Guide.pdf

LPC-Link 2 debug adapter board

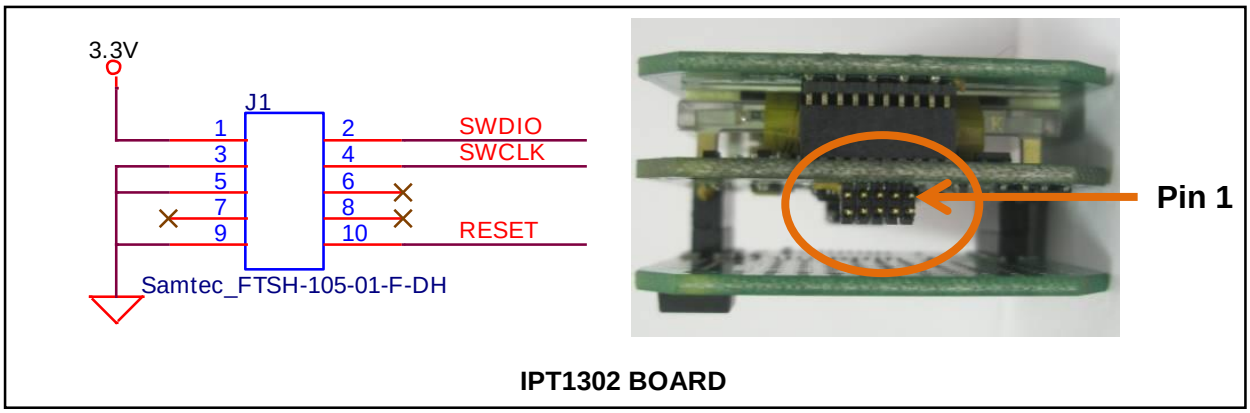
Disconnect “LPC-Link board” from “Target board”



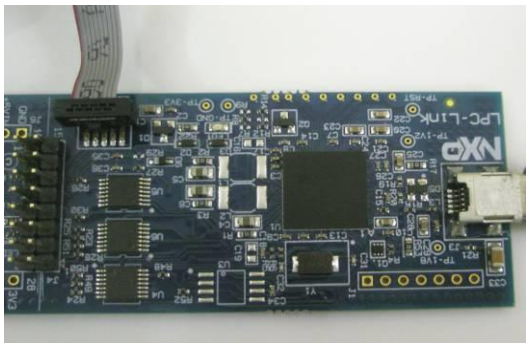
Connect LPC_Link JTAG connector to SmartTool’s J1

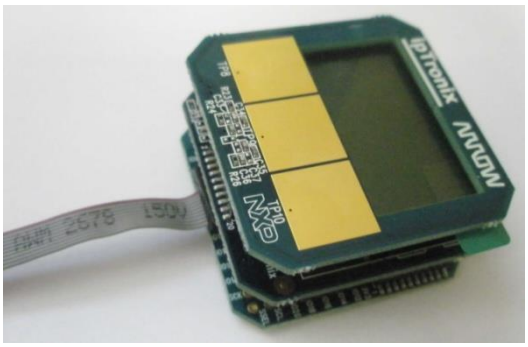


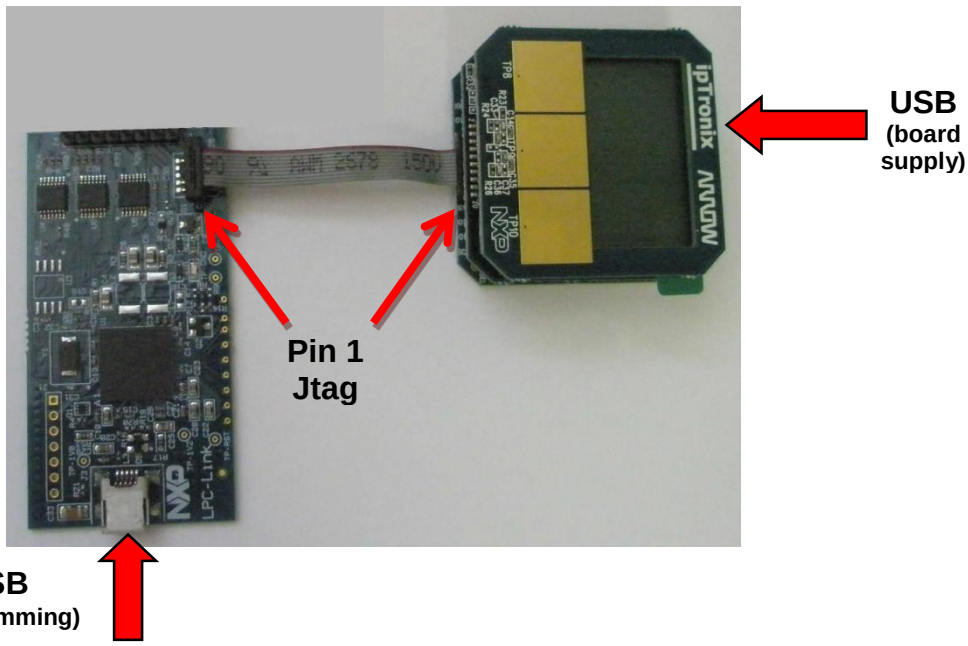
LPC_LINK BOARD



IPT1302 BOARD



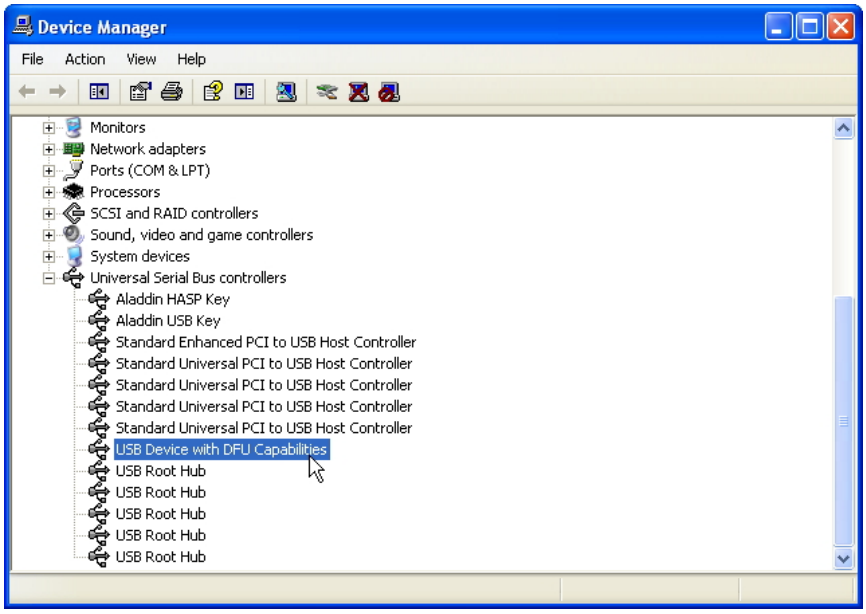




Connect USB cable to SmartTool (power supply)
Connect USB cable to LPC_Link and USB PC port.

When USB cable is connected to LPC_Link for the first time, operating system will prompt for driver installation.

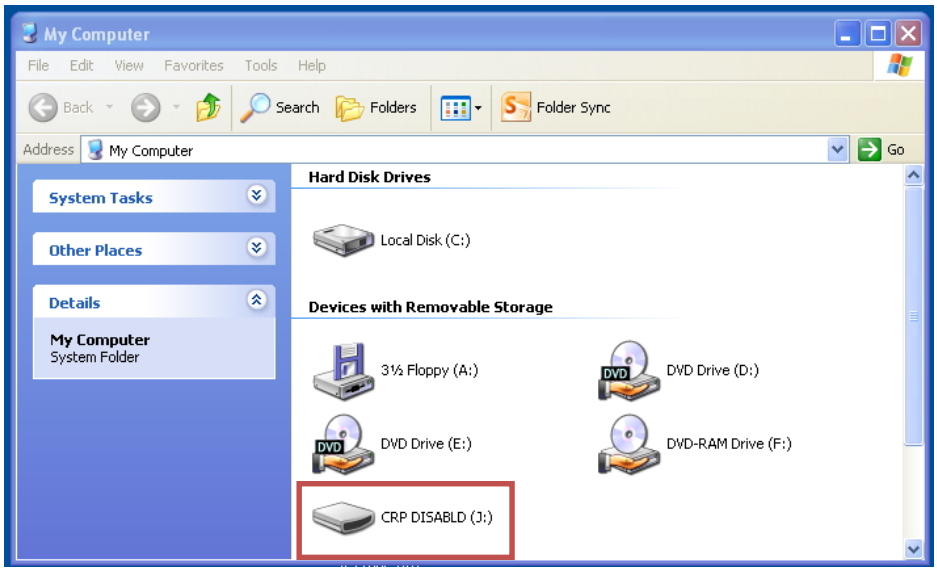
To check that the driver installation was successful, open the Control Panel and check that under USB interface “USB Device with DFU Capabilities” is present.



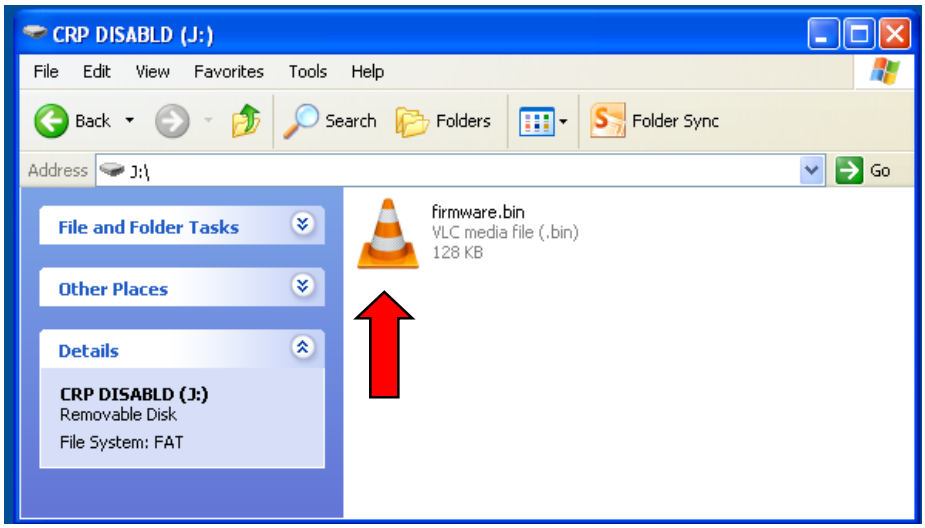
Programming SmartTool from USB

If SmartTool microcontroller is not programmed or application software provides a way to enter ROM bootloader, it’s possible to program the board with .bin app file also without LPCXpresso. To do it, the SmartTool board USB must be connected to the PC.

Open Computer Resources and find “CRP DISABLD” on removable storage device



Open “CRP DISABLD” and replace “firmware.bin“ file with .bin app file you wish to program.



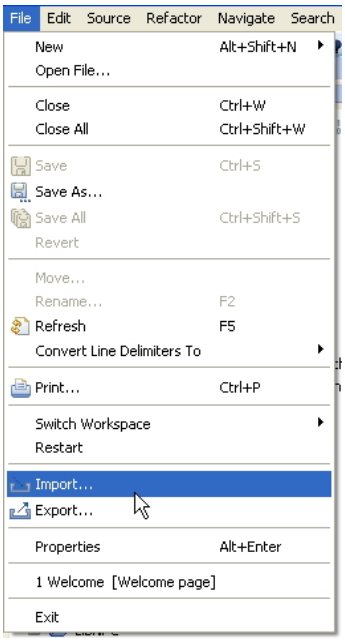
Remove and re-plug USB cable.
At this point downloaded software should run.

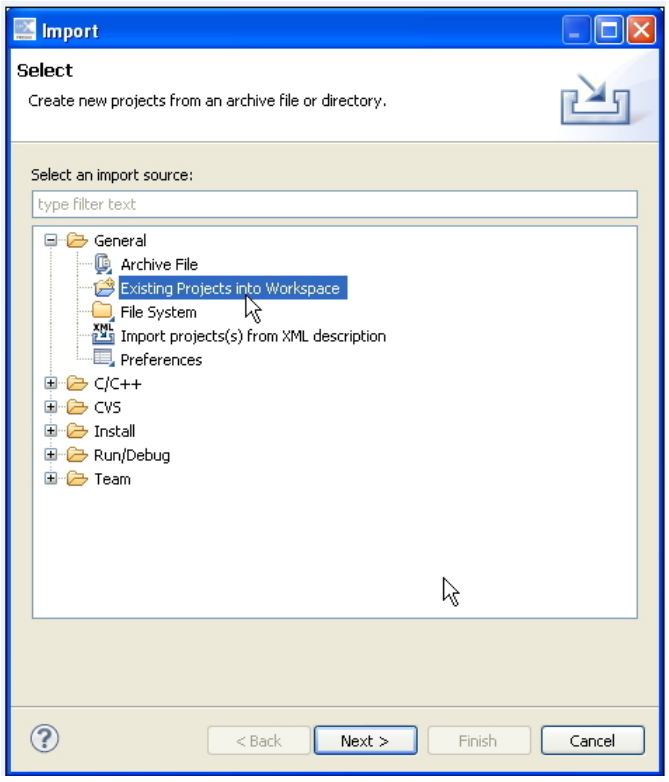
Note

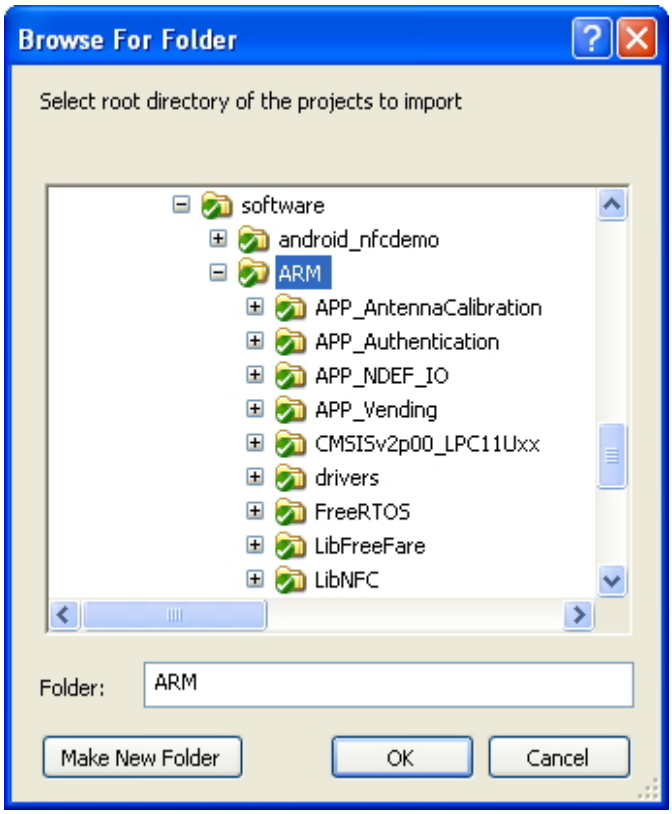
SmartTool comes preprogrammed with the Vending application so this procedure is not applicable unless ROM bootloader is not invoked from the application or the microcontroller is completely erased.

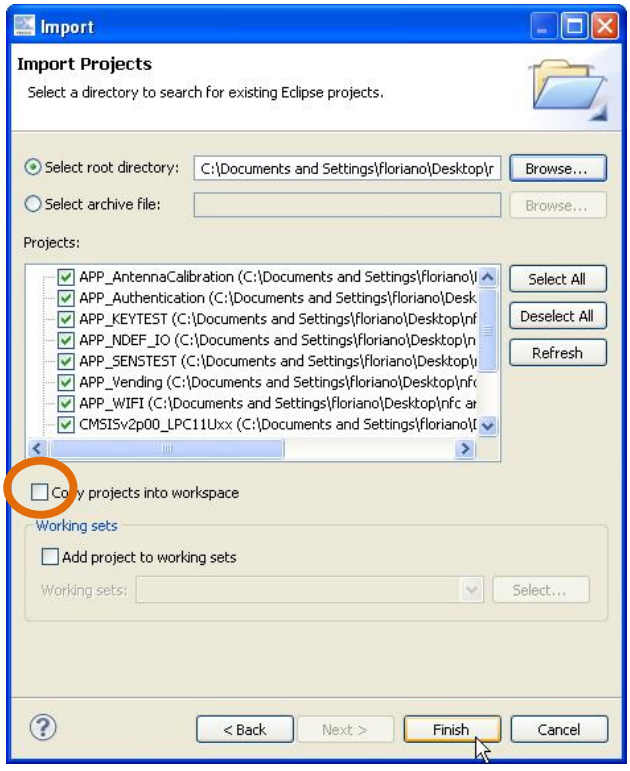
SmartTool programming with LPCXpresso

After running LPCXpresso it's necessary to import the reference design applications in your workspace. In order to do so you have to select import from the file menu.





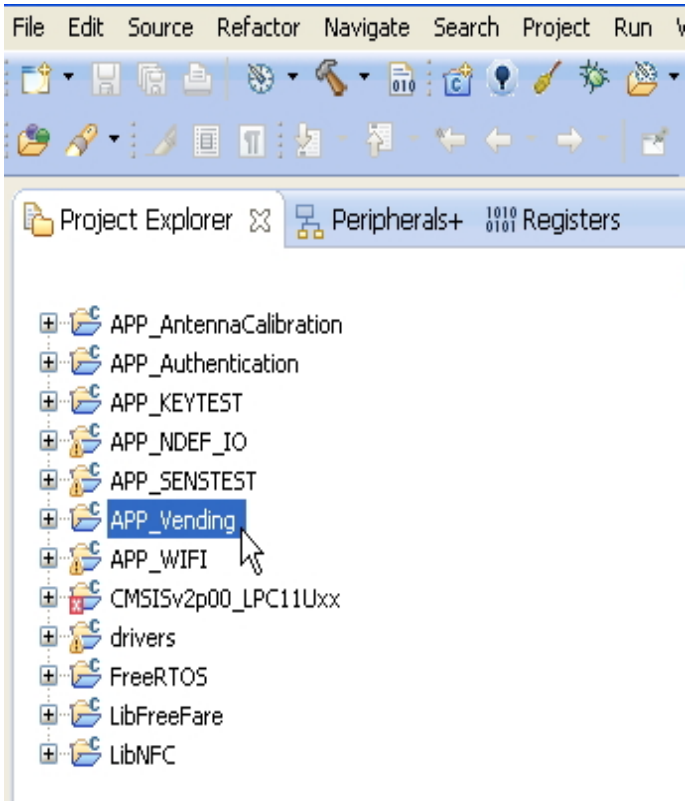




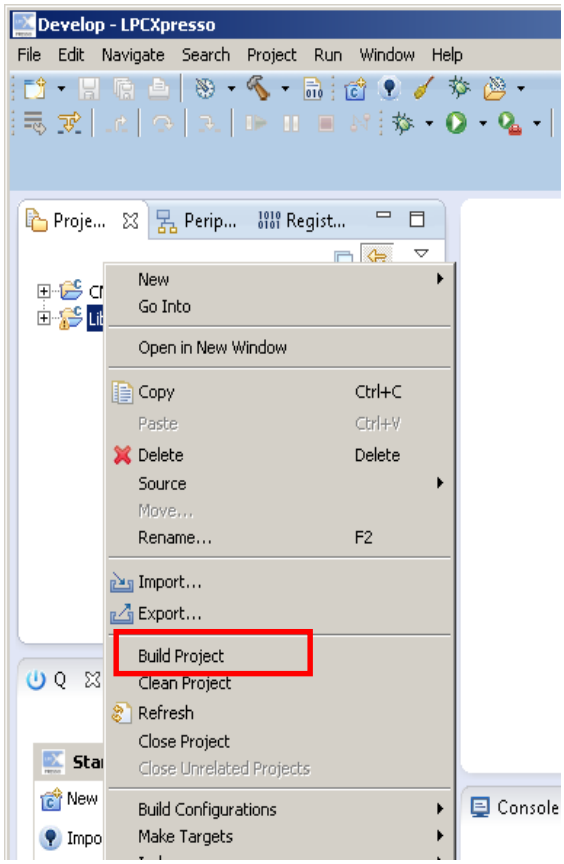
Note

Remove Flag from “Copy project into workspace” if you want to keep project files in the directory they have been originally stored to.

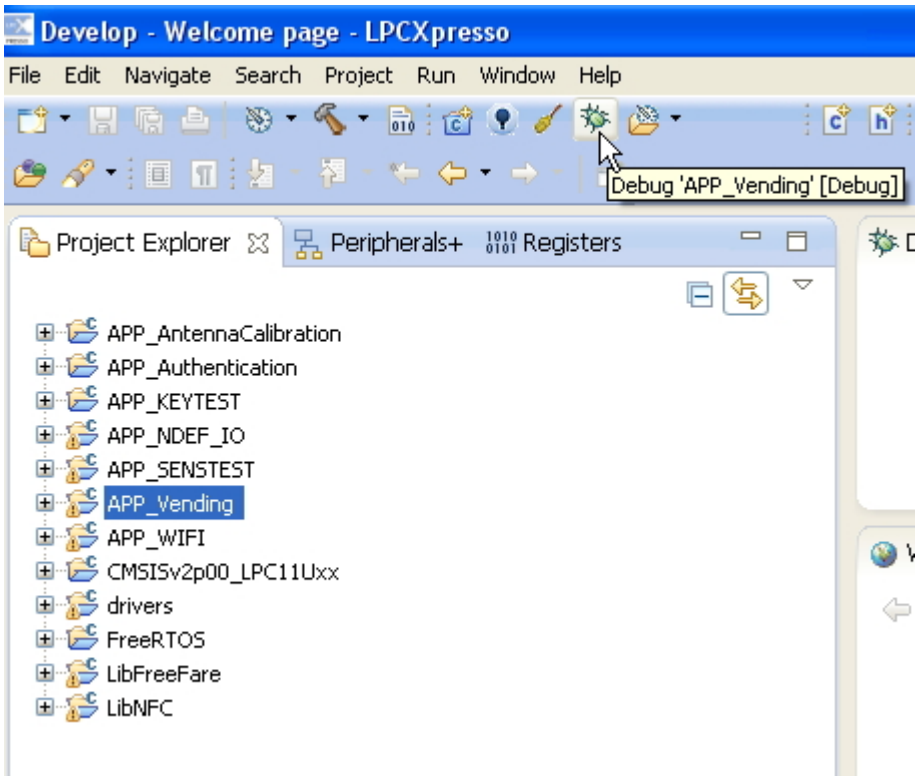
Select with mouse the desired APP,



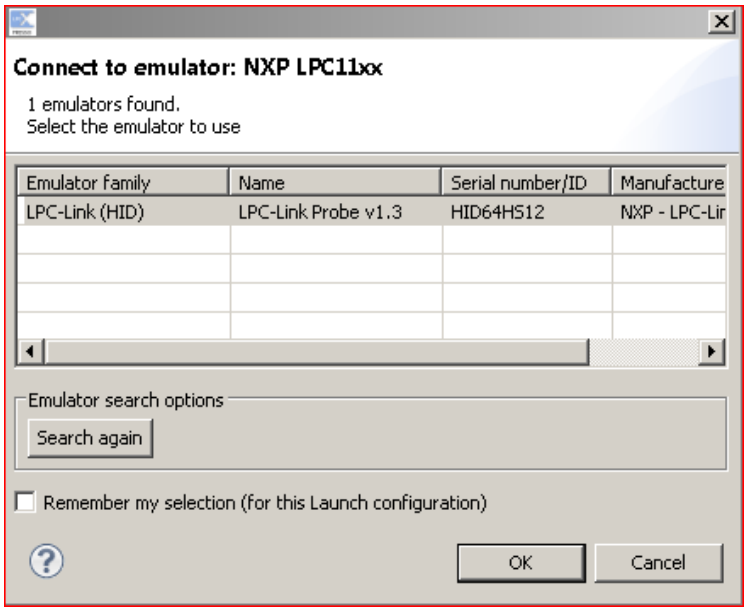
Right bottom mouse click and select “Build Project”



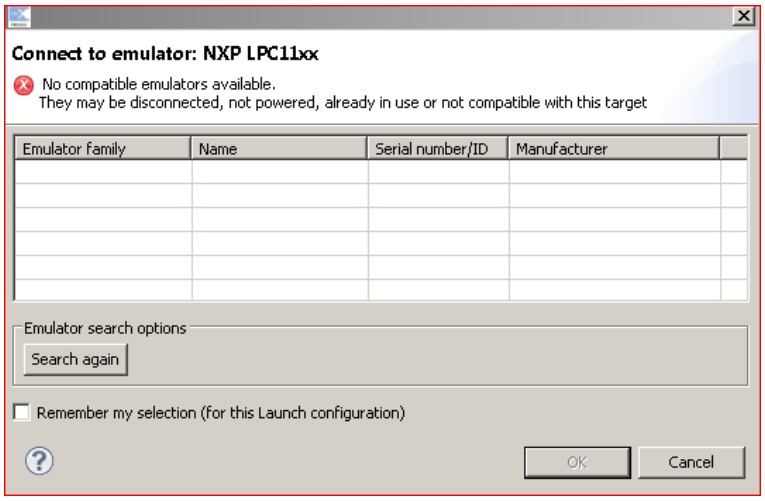
After build is finished, debug firmware with default “Debug” button.

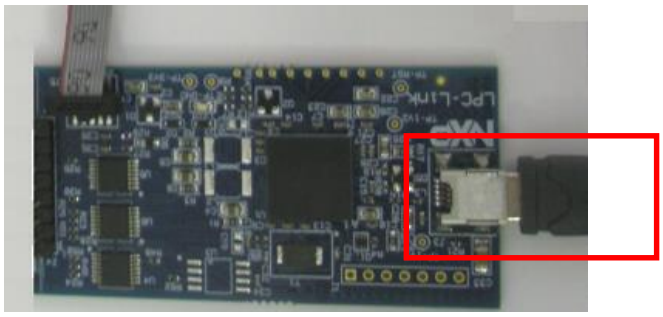


This should bring up the emulator selection window as follows:



In case emulator list is empty try to unplug and re-plug USB cable as often this error comes up due to the debugger being used by a previous debug session.

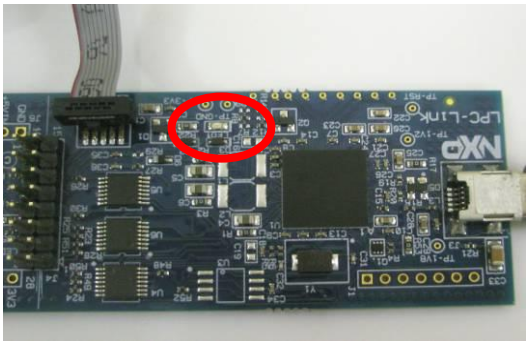




Note

Often this error is displayed if previous debugging sessions have not been terminated by pressing the terminate button

During board programming, Led on LPC-Link board should flash



Note

If you modify files in a library it's always good practice to manually recompile that library as LPCXpresso often doesn't recompile dependent projects.

9 Open Source Software & Modifications

SmartTool software is derived from several open source projects. Since adapting these projects required some modifications a brief description of these projects and what has been changed follows here in after.

FreeRTOS™

FreeRTOS is an operating system optimized for use in embedded/real time applications. The primary objective is to ensure a timely and deterministic response to events. FreeRTOS is professionally developed, strictly quality controlled, robust, supported, and free to use (no upfront payment, no royalties) in commercial products without any requirement to expose your proprietary source code. Commercial support is also available.
See the URL below for more info on FreeRTOS on NXP devices
http://www.lpcware.com/content/project/freertos-nxp-m0-m3-and-m4-mcus

LIBLLCP

libllcp is an implementation of NFC Logical Link Control Protocol (LLCP) for libnfc. This library has not been included in this reference design however it may be interesting to developers who want to implement peer to peer communication. Due to the large amount of memory required by this library, it cannot run on Cortex-M0 devices. It is therefore recommended to select a device with more RAM in case peer to peer is strictly required.
Library can be downloaded from: https://code.google.com/p/libllcp/

LIBNFC

LibNFC is a public, platform independent, NFC library.
LibNFC is a library which provides low level API to handle NFC protocol on a wide variety of transceivers. This library is released under GNU Lesser General Public License. It is completely royalty free and doesn't require linked source code to be released under open source terms.
Original Library can be downloaded from:
https://code.google.com/p/libnfc/source/browse/

Modifications to LibNFC

Library sources used for this reference design have been based on LibNFC version 1.7.0 rc7.

In order to allow LibNFC to run on a resource constrained embedded platform such as SmartTool, memory allocation functions have been replaced with static variables; this imposes a number of limitations such as:

1. LibNFC supports using multiple reader ICs and automatic enumeration; in our version this has been fixed to 1 reader with hardcoded entry. Support for readers different than PN532 has been dropped

2. NFC_STATIC_STRUCTS define has been implemented to remove mallocs and instantiate static variables rather than local (stack allocated) ones. although it's possible to dynamically allocate memory (malloc has been replaced with freeRTOS equivalent), LPC11 memory constraints greatly reduce the possibility to successfully execute especially due to stack size

3. PN532 SPI driver has been modified in order to take advantage of LPC11 hardware platform

4. BUFFER_INIT, BUFFER_APPEND and BUFFER_SIZE macros have been modified to use static variables. These buffers are now statically declared and reuse 2 global buffers rather than using stack allocated variables. The use of buffers statically allocated in memory, makes the functions not reentrant.

LibFreeFare

LibFreeFare provides high level access to Mifare cards. This includes APIs to handle MAD and DESFire cards.
Library can be downloaded from: https://code.google.com/p/libfreefare/

Modifications to LibFreeFare

In order to reduce footprint, remove dynamic memory allocation and make code more embedded friendly the following modifications/restrictions have been imposed to LibFreeFare Port

1. Only selected files have been imported from openSSL. Some headers have been modified to remove OS dependencies

2. Only one tag at time is supported. if more than one tag is detected only the first will be used

OpenSSL

A prerequisite for LibFreeFare is OpenSSL as LibFreeFare uses OpenSSL APIs for AES and DES encryption and decryption. Since OpenSSL is quite big, only the required APIs have been ported and the RAND_bytes function has been directly implemented using rand() from C standard library.

10 SmartTool Software

The SmartTool software package contains libraries, low level drivers and high level applications.

Libraries

The projects below are library files that include low level drivers along with operating system and NFC libraries. This modular approach allows you to quickly swap any of the components or to remove dependency in case this is not needed for your application.

Project	Description
CMSISv2p00_LPC11Uxx	CMSIS library for LPC11Uxx
drivers	Drivers for LPC11 peripherals
FreeRTOS	FreeRTOS operating system files
LibNFC	LibNFC source files
LibFreeFare	LibFreeFare source files

Applications

The following applications that can be loaded on board or customized according to your preferences:

Project	Description
APP_Authentication	Access control sample application
APP_NDEF_IO	NDEF card reader/writer and card emulation sample
APP_Vending	Vending machine sample application

Utilities

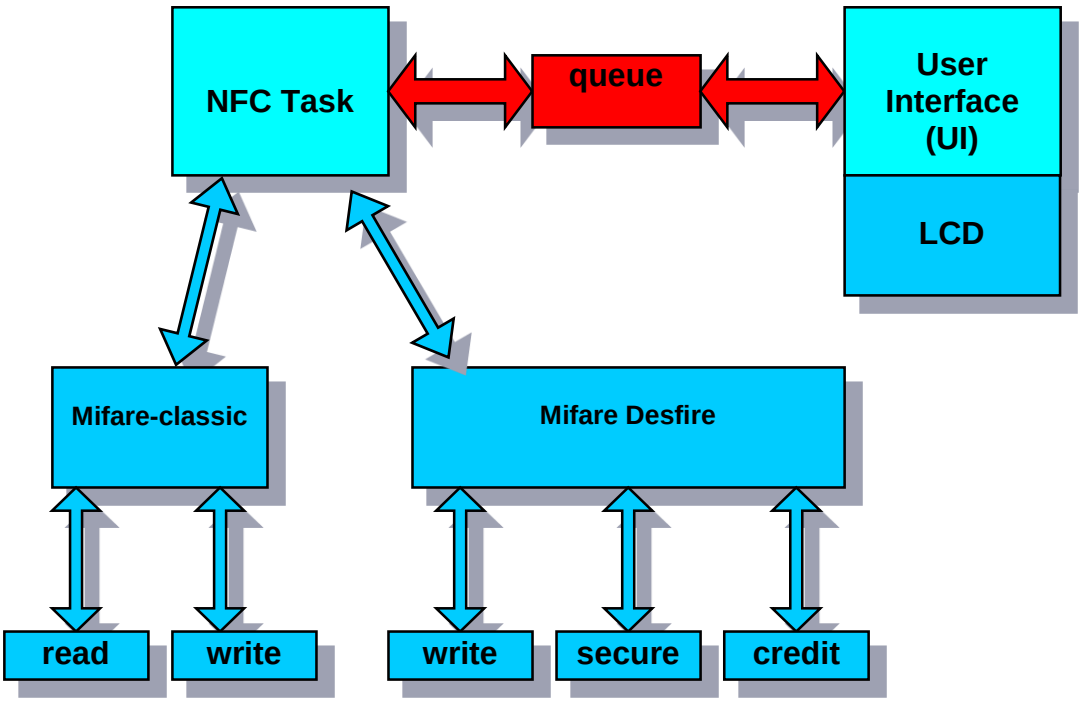
An antenna calibration application is provided to check antenna tuning.

Project	Description
APP_AntennaCalibration	Antenna calibration utility

Application walk through

All applications share a common skeleton and infrastructure.
In each application folder there is main.c file that contains startup and initialization code. The initialization code sets up peripherals, operating system and starts the tasks for the application. Note that FreeRTOS API that start tasks also set up the stack area for each task and that the value provided is in DWORD (4 bytes) units.

Most applications are structured as two tasks that exchange information through a queue:



The UI task generally waits for data from the NFC task executing xQueueReceive(), which holds task for a predefined amount of time or forever in case timeout is set to portMAX_DELAY.
As soon as the NFC task posts data to the queue or queue timeout expires, UI task is woken up and can process received data if any. Eventually the result of this process can be shown on the LCD.
Depending on the kind of application being run, NFC task calls the appropriate APIs through the LibFreeFare or directly through LibNFC libraries.

Note

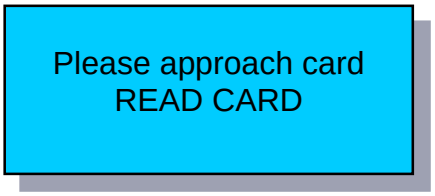
Although Mifare Classic provide security features the reference software intentionally implements secure read/write operations only on DESFire cards as Mifare Classic have been violated and are not suggested for new applications

APP_NDEF_IO

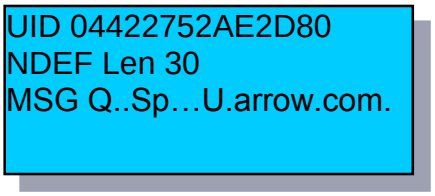
This application shows how to read and write NDEF messages from/to cards and how to exchange NDEF messages with an android cellphone. The project is made up of the following files:

File name	Description
main.c	Peripheral initialization, and UI task implementation
cr_startup_lpc11u.c	Low level startup code
retarget.c	File containing c library hooks functions for printf and malloc implementation
nfc_task.c	File containing NFC task
mifare-classic-read-ndef.c	Utility function implementing NDEF message read from mifare classic cards
mifare-classic-write-ndef.c	Utility function implementing NDEF message write to mifare classic cards
mifare-desfire-read-ndef.c	Utility function implementing NDEF message read from desfire cards
mifare-desfire-write-ndef.c	Utility function implementing NDEF message write to desfire cards
mifare-ultralight-ndef.c	Utility functions to read/write from/to Mifare ultralight cards
nfc-emulate-forum-tag4.c	File containing the functions for NFC card emulation.

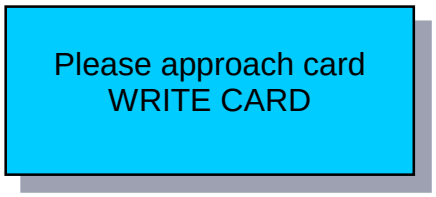
By pressing the left/right buttons the user can cycle between three different operating modes: Read Card Mode ->Write Card Mode -> Emulate Card Mode.
In read Card Mode the system scans for the proximity of a Mifare Classic/Desfire/Ultralight card.



When a valid tag is detected the UID of the tag, the length of the NDEF message and the NDEF message itself will be shown on display.



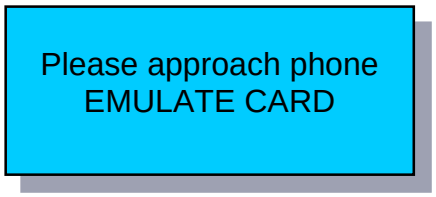
In Write Card Mode, the system scans for a valid tag to write.



As above valid tags are Mifare Classic/Desfire/Ultralight cards. Once a tag is detected an embedded constant NDEF message will be written on tag. This NDEF message consists of a single smart poster record type:

```
const uint8_t ndef_default_msg[32] = {
 0,    30,
    0xd1, 0x02, 0x19, 0x53, 0x70, 0x91, 0x01, 0x0a,
    0x55, 0x01, 0x61, 0x72, 0x72, 0x6f, 0x77, 0x2e,
    0x63, 0x6f, 0x6d, 0x55, 0x00, 0x08, 0x69, 0x70,
    0x54, 0x72, 0x6f, 0x6e, 0x69, 0x78
};
```

This smart poster contains an URI record of value http://www.arrow.com and a binary record of value “ipTronix”. Once the NDEF message has been written into the tag, the message “Write tag ok” will be shown on display.



In Emulate Card Mode, the system emulates a type 4 tag, waiting for an NFC reader/writer device (as a smartphone) to approach. When the NFC device approaches the system, it will read the embedded NDEF message and perhaps will write another NDEF message. Shall this happen, this message will be printed on the LCD together with its length.

APP_Authentication

The application is provided as an example of access control implementation. It is developed only for DESFire (EV1) since the algorithm Crypto1 (used on Mifare Classic) has been cracked; NXP suggest using, in those applications where the security of communications is critical, the MIFARE DESFire (EV1).

The application files are the following:

File name	Description
main.c	Peripheral initialization, and UI task implementation
cr_startup_lpc11u.c	Low level startup code

retarget.c	File containing c library hooks functions for printf and malloc implementation
nfc_task.c	File containing NFC task
mifare-desfire-secure.c	Utility functions implementing secure access to desfire cards
nfc-emulate-forum-tag4.c	File containing the functions for NFC card emulation.

By using the left/right buttons, the user can cycle between three different operating modes: Mode Authorize -> Mode Deny-> Mode Authenticate.
In mode Authorize the system continuously scans for a DesFire tag. Once a DesFire is found the following steps will be executed:

- Select Application with AID equal to 000000h to select the PICC level
- Authentication with PICC master key needed to issue ChangeKeySettings command
- Send Mifare DESFire ChangeKeySetting to change the PICC master key settings
- Create Application with AID equal to 0xF47000, key settings equal to 0x09, NumOfKeys equal to 01h.
- Select the newly created application
- Authenticate with PICC master key (after creation key is blank so we can use PICC key)
- Change key with the one embedded in the code
- Create Data File with FileNo equal to 00h , ComSet equal to 00h and set AccesRights equal to 0000h (master key required for all access)
- The following structure will be then written in the data file (the value of name will be “test” and the value of access_rights will be 0xffffffff):

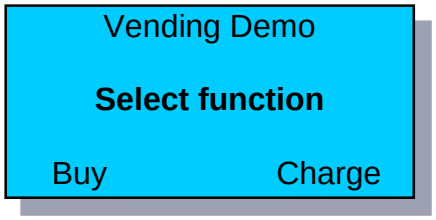
```
typedef struct
{
    char        name[28];
    uint32_t    access_rights;
} secure_payload_sample_t;
```

In mode Deny the same steps described above will be executed, but in the field access_right will be written the value 0.
In mode Authenticate the system will continuously switch between card reader and card emulation mode; if a DesFire tag is detected the system will try to open and read the application with AID equal to 0xF47000. If the file can be opened and the content of the field access_right read from the application file is equal to 0xffffffff, then the mosfet on board will be activated for 1.5 seconds. When in mode Authenticate a NFC device (as a smartphone) approaches the system, it will read the NDEF file which is embedded in the application and will perhaps write another NDEF file. In case the written NDEF file is a smart poster having the URI record set to www.arrow.com and the binary record set to “authenticate”, then the

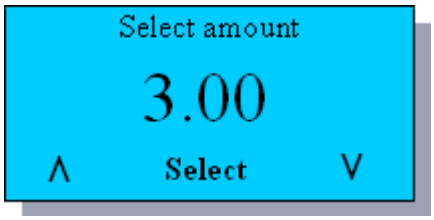
system will consider the authentication valid and will enable the mosfet. Please note that this is not a secure way to handle access control. Everything related to data encryption or whatever is needed to guarantee the security must be implemented by the user in its real case application.

APP_Vending

In order to demonstrate functionality with DesFire tags this app provides easy implementation of access control and credit operations. An application file of the tag will be created and handled to store the user credit. Utility functions contained in the file mifare-desfire-credit.c will be called to increase/decrease the credit.



The application implements a friendly user interface that allows the user to chose between charge the card or buy some good.



In charge mode the user is asked to select the recharge value that will be added to the current credit. After this value is selected the system will scan for a valid tag. Then it will try to access to the credit application file and increase the stored current credit by the selected recharge value. At the end of the operation the LCD will show the total current credit. In buy mode the user can select the item to buy and then approach the card. If the credit file can be opened and the current stored credit is greater than the cost of the selected item to buy, this cost will be subtracted by the current credit value stored in the card. Eventually the updated current credit will be shown on display.

APP_AntennaCalibration

As explained in the chapter **Error! Reference source not found.**, the connector J10 of the HMI board can be connected to the connector J2 of the Main board in two different ways. When J10 is connected to the external row of J2 the antenna on the HMI board is connected to PN532;

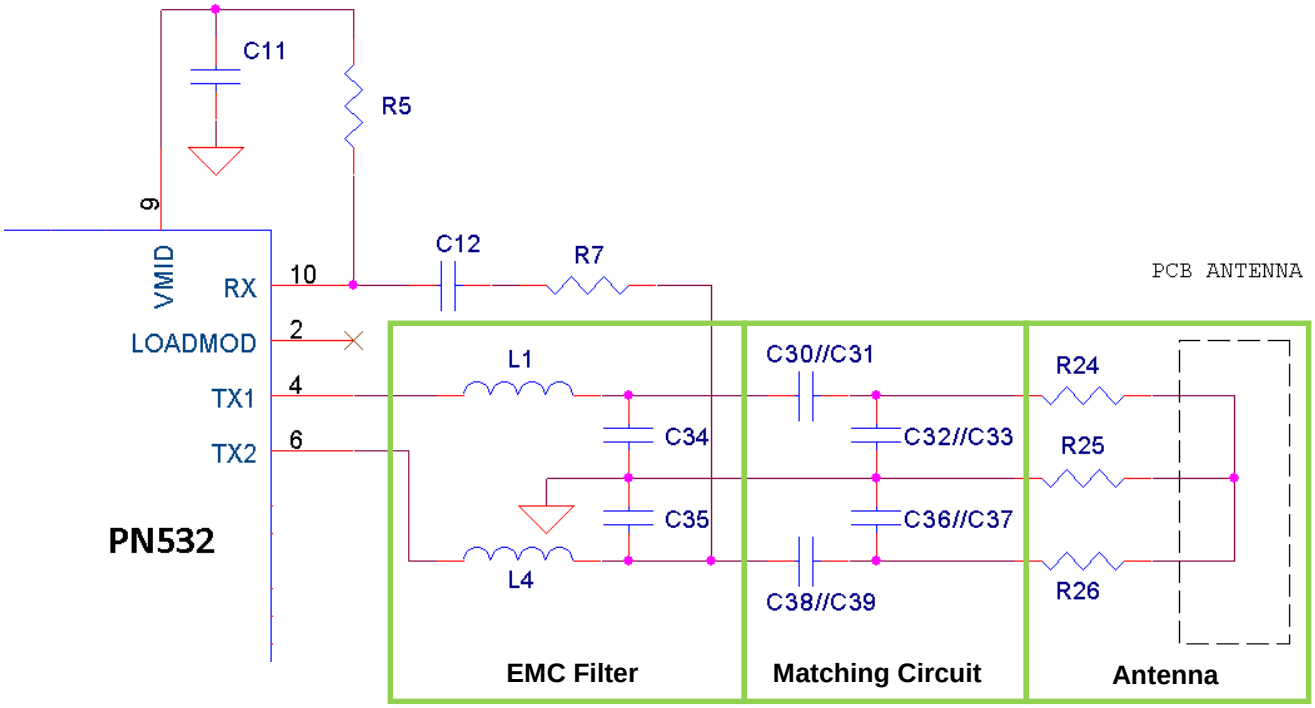
this is the normal mode of the system. If J10 is connected to the internal row of J2, the antenna is connected to the programmable clock generator mounted on the main board; this is the calibration mode of the system. In calibration mode and running the Antenna Calibration Application, a frequency sweep centered on 13.56 MHz will be generated by the clock generator and used to feed the antenna. The ADC of the microcontroller will sample the voltage peak amplitude to the antenna and the result of the conversion will be shown on display. In this way the user can observe the frequency response of the antenna on the LCD, and in case this is not satisfactory, can modify the values of the impedance matching circuit's components (see chapter 11) and retry the sweep, until a good response is achieved.
Please note that by connecting signals directly to the connector J2 of the Main board, the user could use the system to calibrate a different antenna from the one present on the HMI board.

11

Antenna calibration

Several application notes are available on NXP site to give a practical guide to choose the matching component for the PN532 Radio frequency circuit.
The RF circuit consists of 8 capacitors, 2 inductors, 2 resistors and PCB antenna.
These components can be divided in three groups:

- The EMC filter reduces 13,56Mhz harmonics and performs an impedance transformation (L1, L4, C34, C35);
- The matching circuit acts as an a impedance transformation block matches 50 ohm at pins Tx1,Tx2 of PN532 (C30 in parallel to C31,C32 in parallel to C33, C36 in parallel to C33, C38 in parallel to C39;
- The antenna coil generates the magnetic field.

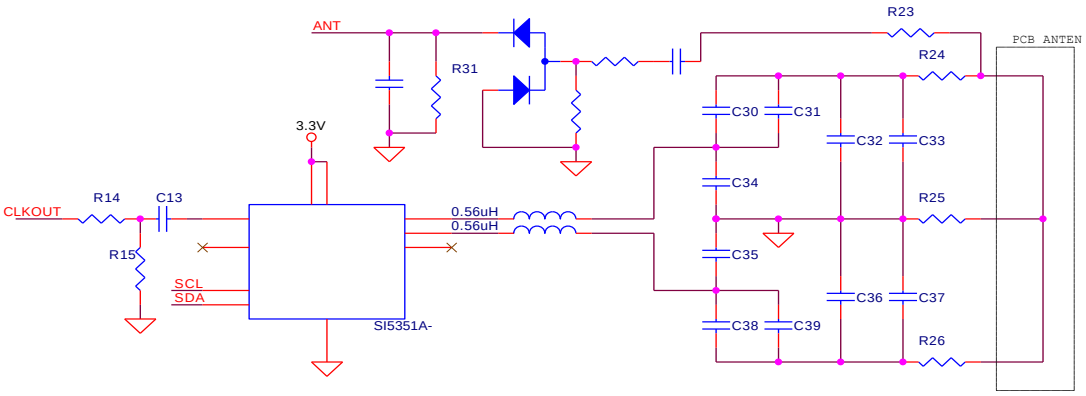


Often the uncertainty of the characteristics of the antenna PCB requires the use of specific tools and instruments (impedance analyzer), to select the values of the RF components.
To help development design, in the IPT1302 board is mounted a simple frequency generator chip (SI5351A-B-GT) that can be used to test the

antenna performances to achieve the best performance for a NFC communication.

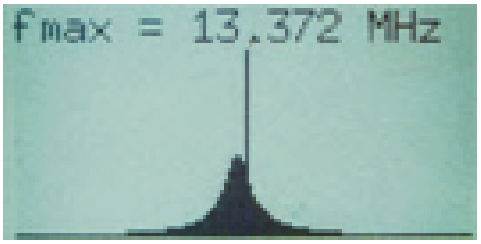
The Antenna calibration app drives Si5351 that is used to feed the antenna with a frequency sweep around desired resonance frequency.

The Si5351 driven, by LPC11U37, with a clock signal through the XA input and configurable through its I2C interface, generate a range of frequency around 13,56MHz.



.

The microprocessors LPC11U37 read analog voltage value on damping resistor and show results on LCD (the maximum peck is the resonance frequency).

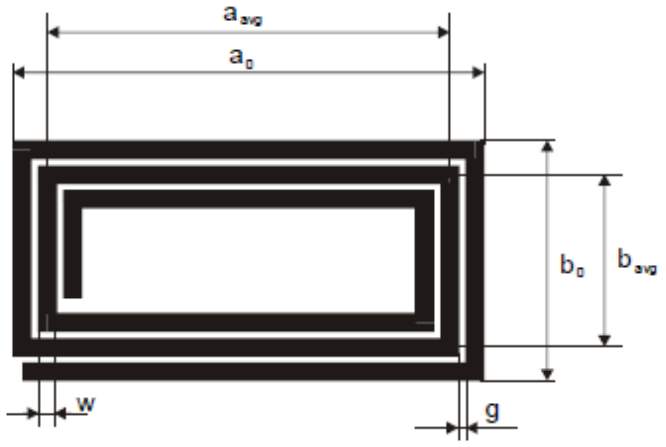


In this way is possible to understand the resonance frequency and after, if necessary, to re-adjust components value to balance antenna value to obtain resonance frequency around 13,56MHz.

Other way can be connecting two scope probes to the ramp generated by the microcontroller and to the antenna and to see the resonance frequency profile of the antenna by simply setting the scope to XY mode.

Antenna PCB theoretical calculation

The inductance can be estimated using the following formula (referenced by AN1445-Antenna design guide for MFRC52X, PN51X and PN53X NXP):



Variables:

a_o, b_o	Overall dimensions of the coil
a_{avg}, b_{avg}	Average dimensions of the coil
t	Track thickness
w	Track width
g	Gap between tracks
N_a	Number of turns
d	Equivalent diameter of the track

The inductance can be calculated by:

$$L_a = \frac{\mu_0}{\pi} \cdot [x_1 + x_2 - x_3 + x_4] \cdot N_a^{1.8}$$

With:

$$d = \frac{2 \cdot (t + w)}{\pi}$$

$$a_{avg} = a_o - N_a \cdot (g + w) \qquad b_{avg} = b_o - N_a \cdot (g + w)$$

$$x_1 = a_{avg} \cdot \ln\left[\frac{2 \cdot a_{avg} \cdot b_{avg}}{d \cdot \left(a_{avg} + \sqrt{a_{avg}^2 + b_{avg}^2}\right)}\right] \qquad x_2 = b_{avg} \cdot \ln\left[\frac{2 \cdot a_{avg} \cdot b_{avg}}{d \cdot \left(b_{avg} + \sqrt{a_{avg}^2 + b_{avg}^2}\right)}\right]$$

$$x_3 = 2 \cdot \left[a_{avg} + b_{avg} - \sqrt{a_{avg}^2 + b_{avg}^2}\right] \qquad x_4 = \frac{a_{avg} + b_{avg}}{4}$$

For example in this PCB, with

Diameter D= 38,1 mm

Antenna width s = 0,5mmq

Number of turns N= 4

the antenna inductance L is 1,45uH.

Other formula calculations are available on internet.

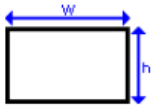
For example:

http://www.ekswai.com/nfc.htm

http://www.technick.net/public/code/cp_dpage.php?aiocp_dp=util_inductance_rectangle

Inductance Calculations: Rectangular Loop

Loop of wire with rectangular shape



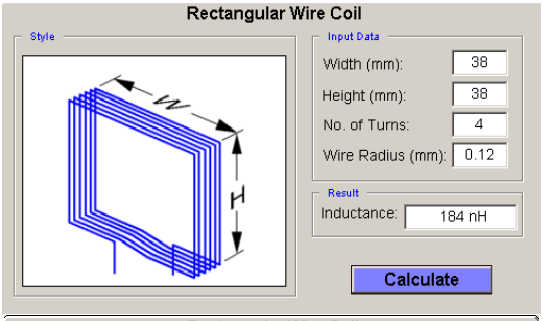
N	4	**[ ]**	number of turns
w	0.038	**[m]**	width of the rectangle
h	0.038	**[m]**	height of the rectangle
a	0.005	**[m]**	wire radius
μ_r	1	**[ ]**	relative permeability of the medium
L	6.100114601192928e-7	**[H]**	Inductance

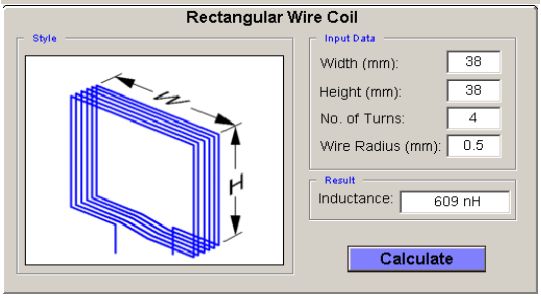
Calculate Clear

NOTE: numbers are in scientific notation (e.g.: 1.427e-9 H = $1.1427 \cdot 10^{-9}$ H = 1.427 nH)

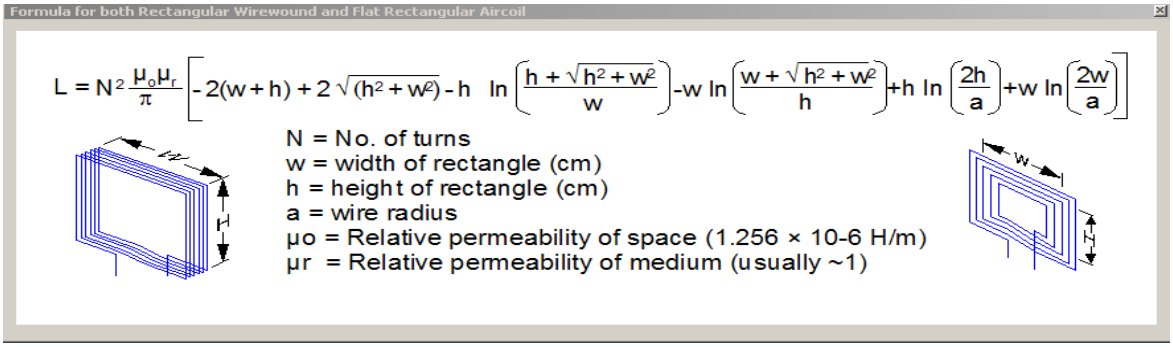
$$L_{rect} \approx N^2 \frac{\mu_0 \mu_r}{\pi}\left[-2(w+h)+2\sqrt{h^2+W^2}-h\ln\left(\frac{h+\sqrt{h^2+W^2}}{W}\right)-W\ln\left(\frac{W+\sqrt{h^2+W^2}}{h}\right)+h\ln\left(\frac{2h}{a}\right)+W\ln\left(\frac{2W}{a}\right)\right]$$

A Texas Instrument tool also are available:





Or NXP formule can be used.



For additional information also refer to [14] [15] [16] [17].

Antenna impedance measure with oscilloscope

Remark:
The complete tuning of a 50 Ω antenna using only an oscilloscope is not as precise as the tuning with an impedance analyzer.
It is recommended to do the first tuning of the antenna with an analyzer and not with an oscilloscope.

The necessary equipment is shown in following figure.

A reference resistor of 50 Ω– 2% (e.g. 50 Ω BNC terminating resistor) is inserted in the ground line between the function generator output and the antenna connector.

The two probes of the oscilloscope are connected to the function generator output and in parallel to the reference resistor.
The components Cy-probe and Cx-probe present the oscilloscope probe input capacitance.

The oscilloscope will display a Lissajous figure, allowing deriving the absolute magnitude and the phase. The magnitude is given by the angle of the Lissajous figure and the area as depicted in the figure below gives the phase.

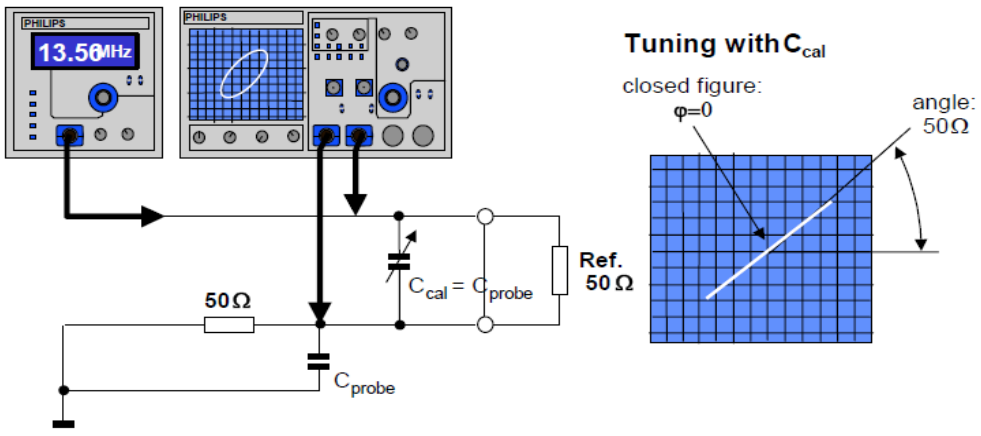
The tuning procedure has to be done in two steps:

Step 1: Setup and Calibration

For the calibration, a resistance of 50 Ω has to be inserted instead of the antenna. The calibration procedure is depicted in the next figure.

The function generator shall be set to:

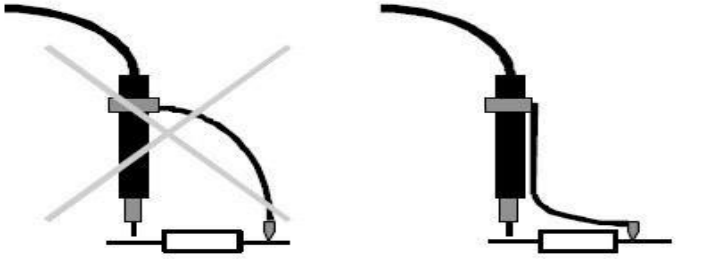
Wave form:	Sinusoidal
Frequency:	13.56 MHz
Amplitude:	2V – 5V
Scale:	scale for the x-probe is chosen twice the scale for the y-probe (e.g. x-scale: 2V/DIV and y-scale: 1V/DIV) so the Lissajous figure angle shall be 45 degree



Simple impedance measurement, calibration

The x-probe capacitance Cxprobe only reduces the amplitude at the function generator output. This has no influence on the tuning results. The y-probe capacitance Cyprobe affects a phase shift, which changes the area of the Lissajous figure. To compensate this effect, the capacitor Ccal is connected in parallel to the matching network.

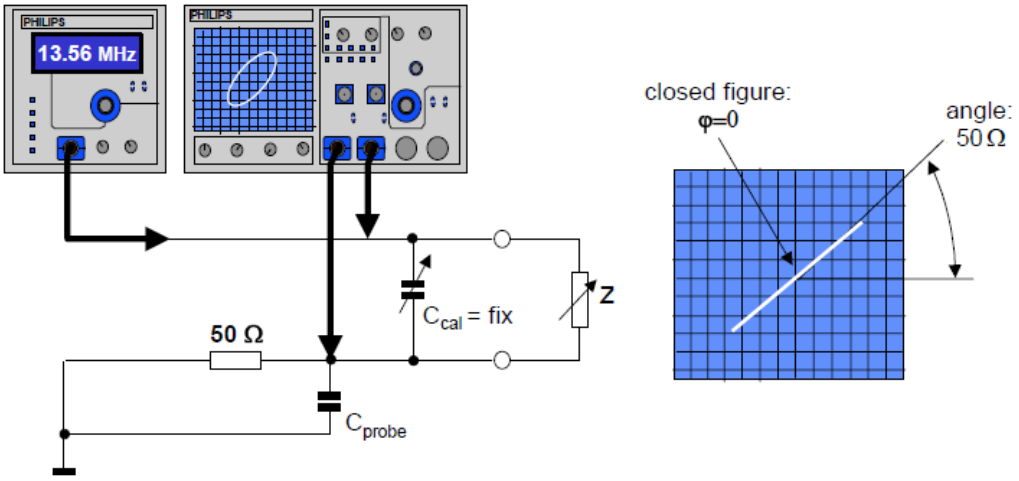
Remark: A loop of the ground cable of the probe shall be avoided to minimize inductive coupling from the antenna.



The x-probe capacitance Cxprobe reduces only the amplitude at the function generator output. This has no influence on the tuning results. The y-probe capacitance Cy probe affects a phase shift, which changes the area of the Lissajous figure.
To compensate this effect, the capacitor Ccal is connected in parallel to the matching network. In the calibration phase the matching network is replaced with a second resistor of 50 Ω (e.g. 50 Ω BNC terminating resistor).
The calibration capacitor has to be adjusted until the Lissajous figure is completely closed. Then the calibration capacitance Ccal is equal to the capacitance Cy-probe. The y-probe voltage is in phase and the amplitude is exactly half of the function generator voltage (x-probe).

Step 2: TUNING PROCEDURE:

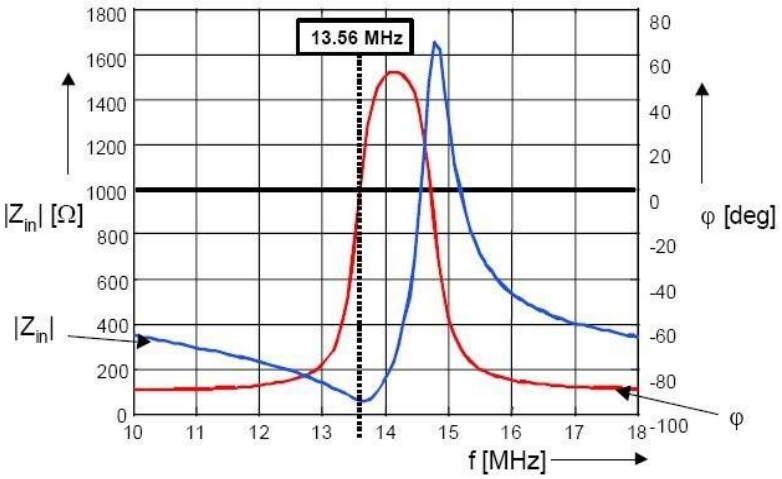
After the calibration, the calibration resistor has to be replaced by the antenna. The matching network shall be tuned by the variable capacitor C30/C31 (same C38/C39s and C32//C33 (same C36//C37) until the Lissajous figure is completely close.
The Lissajous figure angle has to be compared to the Lissajous figure angle of the calibration resistor.
If the angle is equal to the angle of the calibration resistor, the matching circuit impedance is 50 Ω.



Notes to interpret the Lissajous figures:.

If the figure is not closed the phase between x and y is unequal to zero.
If the angle j=0°, the Lissajous figure is closed completely.
If the angle is greater than 45°, Z is greater than 50 Ω.
If the angle is smaller than 45°, Z is greater than 50 Ω

The resonance curve of an antenna has two zeros in the phase as shown in figure:

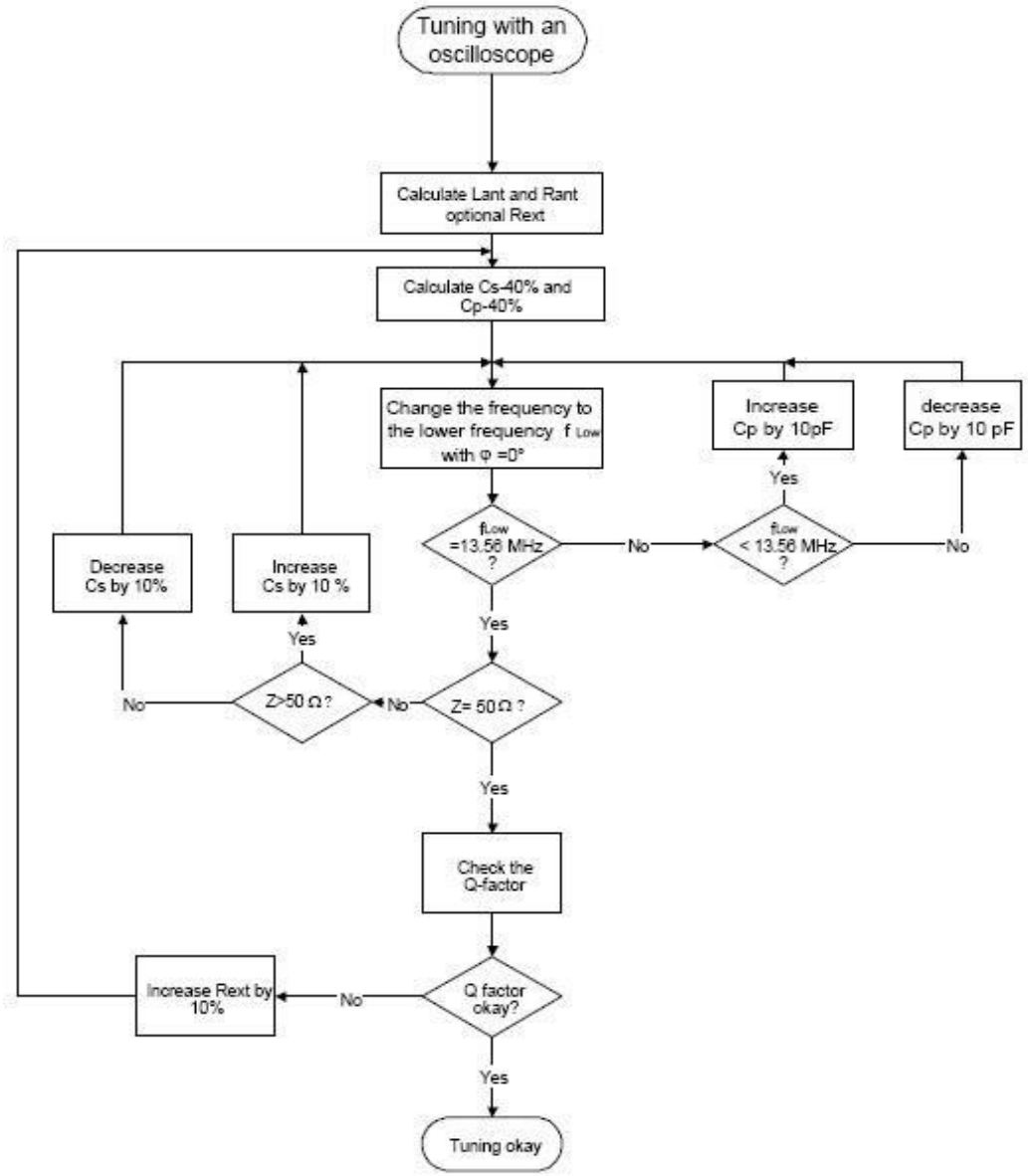


Input impedance and phase of a tuned circuit

It is only possible to tune the lower frequency F_{LOW} to Z=50 Ω and j= 0°. The zero at the higher frequency can not be tuned to Z=50 Ω.

To be sure that the tuning is done to the lower frequency, it is recommended to reduce the calculated value for C30/C31 (same C38/C39s and C32//C33 (same C36//C37) by 40% and add tuning capacitors in that range. Start the tuning with the lowest values for the tuning capacitors.

The complete tuning procedure is described as a flow chart in Figure 8.



Cs= C30/C31 (same C38/C39
Cp= C32//C33 (same C36//C37)

Frequency versus application: recommendations

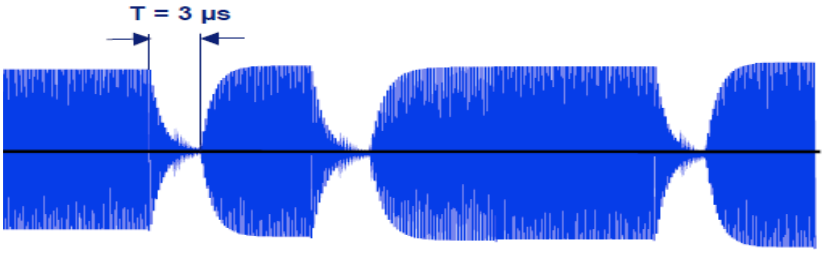
Before designing the tag antenna it is important to know which frequency has to be used in your application:

- *Long-range (LR) products are usually tuned between 13.6 MHz and 13.7 MHz (for distance optimization).*
- *Standard short-range SR products are usually tuned between 13.6 MHz and 13.9 MHz (for distance optimization).*
- *Short-range products used as transport tickets are usually tuned between 14.5 MHz and 15 MHz (for stack optimization).*

These targeted frequencies should take into account the frequency shift due to the final label material and environment.
For example on a sticker tag with a paper label it's necessary to tune the initial inlay at about 13.9 MHz instead of the specified 13.6 MHz because the paper and adhesive decrease the inlay antenna frequency by about 300 kHz.

Checking Q-Factor

The performance of an antenna is related with its Quality (Q) factor and is a determining constraint to design and tune an antenna because maximum timing limit of 3us (as defined in the ISO/IEC14443) for a modulation pause is taken to calculate the quality factor.



Pulse width definition

This picture shows an excerpt of a typical 100% ASK modulation.

The bandwidth B –pulse width T product is defined as:

$$B * T \geq 1$$

With the bandwidth definition

$$B = \frac{f}{Q}$$

the B-T product results to

$$Q \leq f \cdot T$$
$$Q \leq 13.56MHz \cdot 3\mu s$$
$$Q \leq 40.68$$

Note: The recommended antenna quality factor is Q = 35.

So, when design a NFC reader antenna, the Q-factor has to be checked. The quality factor of the antenna loop can be calculated using the following equation:

$$Q = \frac{2 \times \pi \times f_0 \times L_R}{R_{LR}}$$

Where:

L_R is the inductance of reader antenna

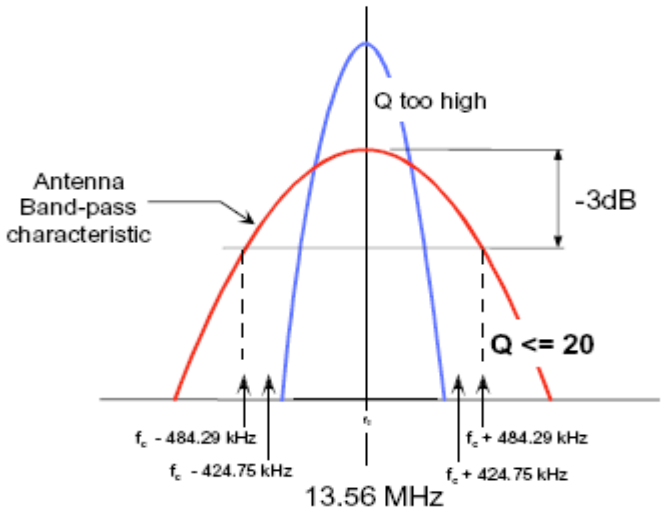
R_{LR} is the natural resistance of the reader antenna

f_0 is the resonant frequency in MHz

The overall Q-factor of a NFC antenna, supporting higher bit rates is limited to

$$Q \leq 35 \quad (\text{recommended value is} = 35)$$

If a LCR measurement instruments is not available, to measure the Q-factor can be use an oscilloscope.
With the oscilloscope, the maximum voltage is recorded as the frequency is adjusted and this value multiplied by 0.707 in order to obtain the equivalent -3dB value.



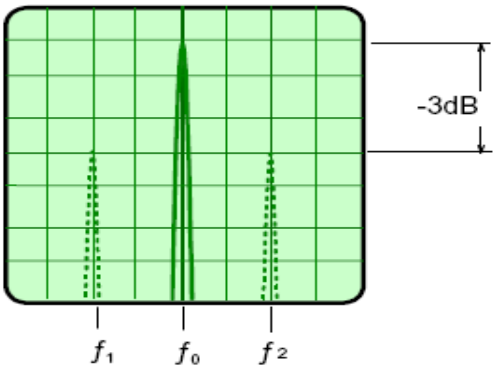


Figure 11. Spectrum Analyzer screen

The frequency is then raised and lowered to get the $f1$ and $f2$ values.

The Q value is:

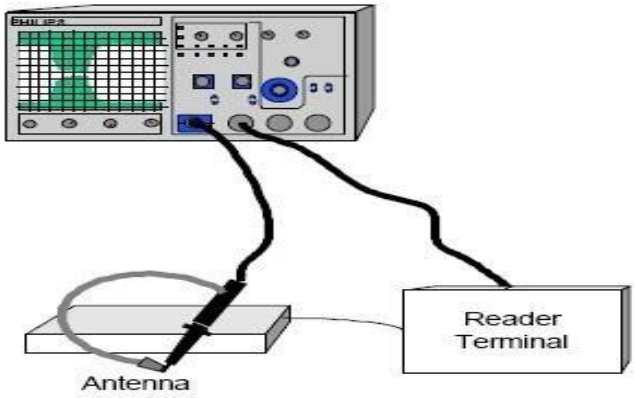
$$Q = \frac{f_0}{f_2 - f_1}$$

The overall Q-factor of a NFC antenna, supporting higher bit rates is limited to $Q \leq 35$.
For additional information also refer to [14] [15] [16] [17].

Pulse shape check

The following pulse shape checks are a quick way for investigating the shaping of the generated RF-field. In addition to verifying the correspondence of the transition to the standard ISO/IEC 18092 also allows to check the Q-factor because the Q-factor has a direct influence on the edges of the modulation shape.

An oscilloscope with a bandwidth of at least 50 MHz has to be used and two probes have to be connected as shown below:

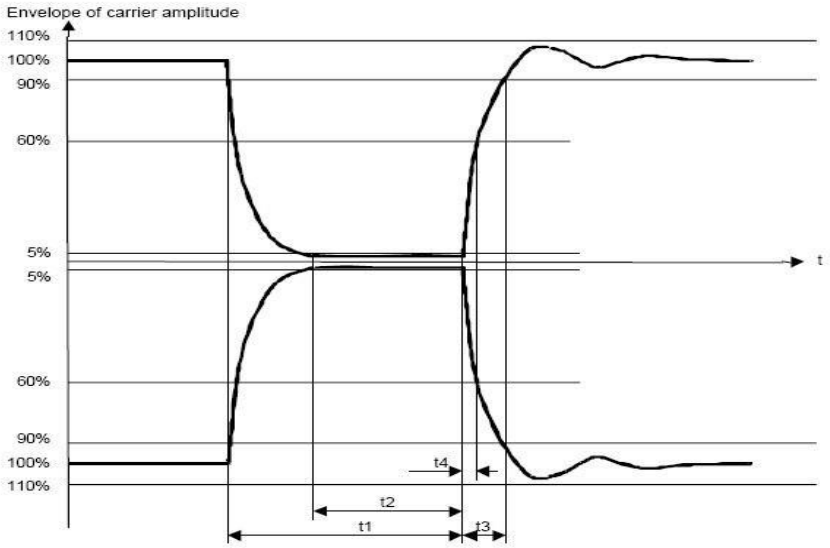


Setup to check the Q-factor

The probes have to be connected in the following way:

CH1: Form a loop with the ground line at the probe to enable inductive signal coupling. Hold the probe loop closely above the antenna.
CH2: Connect probe to the NPAUSE0 signal in your MIFARE reader, (it is used for easy triggering) Trigger source = CH2.

To check the pulse shape it is recommended to compare the plot on the scope to Figure below. The values can be found in following table



Pulse shape definitions according to ISO/IEC18092, 106 kbps

Pulse length (Condition)	t1 [µs]	t2 [µs] (t1 ≤ 0,5)	t2 [µs] (t1 > 2,5)	t3 [µs]	t4 [µs]
Maximum	3,0	t1		1,5	0,4
Minimum	2,0	0,7	0,5	0,0	0,0

To check the correct tuning the time t2 is of special interest.
This time describes the time span, in which the signal falls under the 5 % value of the 90% value of the amplitude of the signal.

For a correct tuning of antenna especially for a correct value of the external resistance REXT (R24-R25) the following has to be fulfilled:

- The signal has to fall under the 5% value
- The time t2 should not exceed 1.4µs.

If t2 is greater than 1,4µs the Q-factor is greater than 35 and the correct data transmission cannot be guaranteed. Increase REXT(R24-R25).
If the time t2 is shorter than 0,7µs the Q-factor is too high and the operating distance will be dissatisfying. Decrease REXT(R24-R25).

For additional information also refer to [14] [15] [16] [17].

12 SmartTool design files

Schematics

Schematic diagrams are provided in PDF (Adobe Acrobat) and .DSN (Orcad Capture 7.2) file formats.

PCB

PCB files are provided in the following formats:

File extension	Description
.pcb	Mentor Graphics PADS PowerPCB version 9.5 binary file
.asc	Mentor Graphics PADS PowerPCB version 5.0.1 ascii file
gerber	Fabrication files in 274X format, including drill and SMT placement files. Includes also PDF files for review
.emn/.emp	Generic 3D IDF3.0 Format for 3d modeling
.fcstd	Freecad 3D model

BOM

BOM is provided in Microsoft excel format.