WIRELESS POWER CONSORTIUM

Qi Specification

NFC/RFID Card Protection (Informative)

Version 1.3

January 2021

COPYRIGHT

DISCLAIMER

The information contained herein is believed to be accurate as of the date of publication, but is provided "as is" and may contain errors. The Wireless Power Consortium makes no warranty, express or implied, with respect to this document and its contents, including any warranty of title, ownership, merchantability, or fitness for a particular use or purpose. Neither the Wireless Power Consortium, nor any member of the Wireless Power Consortium will be liable for errors in this document or for any damages, including indirect or consequential, from use of or reliance on the accuracy of this document. For any further explanation of the contents of this document, or in case of any perceived inconsistency or ambiguity of interpretation, contact: info@wirelesspowerconsortium.com.

RELEASE HISTORY

Specification Version	Release Date	Description
1.3	January 2021	Initial release of this document.

Table of Contents

1 General

The Wireless Power Consortium (WPC) is a worldwide organization that aims to develop and promote global standards for wireless power transfer in various application areas. A first application area comprises flat-surface devices such as mobile phones and chargers in the Baseline Power Profile (up to 5 W) and Extended Power Profile (above 5 W).

1.1 Structure of the Qi Specification

General documents

- Introduction
- Glossary, Acronyms, and Symbols

System description documents

- Mechanical, Thermal, and User Interface
- Power Delivery
- Communications Physical Layer
- Communications Protocol
- Foreign Object Detection
- NFC/RFID Card Protection
- Authentication Protocol

Reference design documents

- Power Transmitter Reference Designs
- Power Receiver Design Examples

Compliance testing documents

- Power Transmitter Test Tools
- Power Receiver Test Tools
- Power Transmitter Compliance Tests
- Power Receiver Compliance Tests

NOTE: The compliance testing documents are restricted and require signing in to the WPC members' website. All other specification documents are available for download on both the WPC public website and the WPC website for members.

1.2 Scope

The *Qi Specification, NFC/RFID Card Protection (Informative)* (this document) provides guidelines (informative) for detecting the presence of a Radio Frequency Identification (RFID) tag or Near Field Communication (NFC) card within the operating range of the Power Transmitter and preventing damage to the tag or card.

1.3 Compliance

All provisions in the *Qi Specification* are mandatory, unless specifically indicated as recommended, optional, note, example, or informative. Verbal expression of provisions in this Specification follow the rules provided in ISO/IEC Directives, Part 2.

Table 1: Verbal forms for expressions of provisions

Provision	Verbal form
requirement	"shall" or "shall not"
recommendation	"should" or "should not"
permission	"may" or "may not"
capability	"can" or "cannot"

1.4 References

For undated references, the most recently published document applies. The most recent WPC publications can be downloaded from http://www.wirelesspowerconsortium.com. In addition, the *Qi Specification* references documents listed below. Documents marked here with an asterisk (*) are restricted and require signing in to the WPC website for members.

- Product Registration Procedure Web page*
- Qi Product Registration Manual, Logo Licensee/Manufacturer*
- Qi Product Registration Manual, Authorized Test Lab*
- Power Receiver Manufacturer Codes,* Wireless Power Consortium
- The International System of Units (SI), Bureau International des Poids et Mesures
- Verbal forms for expressions of provisions, International Electotechnical Commission

For regulatory information about product safety, emissions, energy efficiency, and use of the frequency spectrum, visit the regulatory environment page of the WPC members' website.

1.5 Conventions

1.5.1 Notation of numbers

- Real numbers use the digits 0 to 9, a decimal point, and optionally an exponential part.
- Integer numbers in decimal notation use the digits 0 to 9.
- Integer numbers in hexadecimal notation use the hexadecimal digits 0 to 9 and A to F, and are prefixed by "0x" unless explicitly indicated otherwise.
- Single bit values use the words ZERO and ONE.

1.5.2 Tolerances

Unless indicated otherwise, all numeric values in the *Qi Specification* are exactly as specified and do not have any implied tolerance.

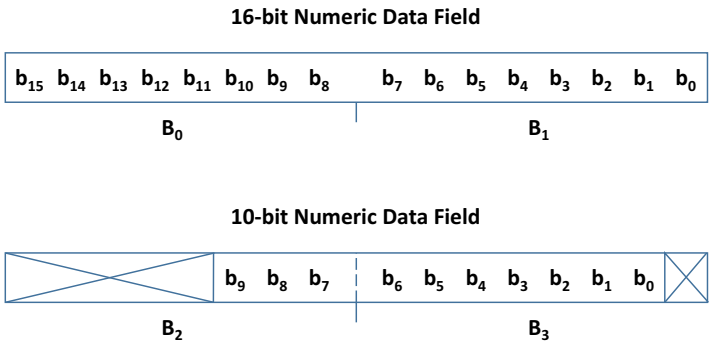
1.5.3 Fields in a data packet

A numeric value stored in a field of a data packet uses a big-endian format. Bits that are more significant are stored at a lower byte offset than bits that are less significant. Table 2 and Figure 1 provide examples of the interpretation of such fields.

Table 2: Example of fields in a data packet

	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0
B_0	(msb) 16-bit Numeric Data Field							
B_1								(lsb)
B_2	Other Field					(msb)		
B_3	10-bit Numeric Data Field						(lsb)	Field

Figure 1. Examples of fields in a data packet



1.5.4 Notation of text strings

Text strings consist of a sequence of printable ASCII characters (i.e. in the range of 0x20 to 0x7E) enclosed in double quotes ("). Text strings are stored in fields of data structures with the first character of the string at the lowest byte offset, and are padded with ASCII NUL (0x00) characters to the end of the field where necessary.

EXAMPLE: The text string “WPC” is stored in a six-byte fields as the sequence of characters 'W', 'P', 'C', NUL, NUL, and NUL. The text string “M:4D3A” is stored in a six-byte field as the sequence 'M', ':', '4', 'D', '3', and 'A'.

1.5.5 Short-hand notation for data packets

In many instances, the *Qi Specification* refers to a data packet using the following shorthand notation:

<MNEMONIC>/<modifier>

In this notation, <MNEMONIC> refers to the data packet's mnemonic defined in the *Qi Specification, Communications Protocol*, and <modifier> refers to a particular value in a field of the data packet. The definitions of the data packets in the *Qi Specification, Communications Protocol*, list the meanings of the modifiers.

For example, EPT/cc refers to an End Power Transfer data packet having its End Power Transfer code field set to 0x01.

1.6 Power Profiles

A Power Profile determines the level of compatibility between a Power Transmitter and a Power Receiver. Table 3 defines the available Power Profiles.

- *BPP PTx*: A Baseline Power Profile Power Transmitter.
- *EPP5 PTx*: An Extended Power Profile Power Transmitter having a restricted power transfer capability, i.e. $P_L^{(pot)}$ = 5 W.
- *EPP PTx*: An Extended Power Profile Power Transmitter.
- *BPP PRx*: A Baseline Power Profile Power Receiver.
- *EPP PRx*: An Extended Power Profile Power Receiver.

Table 3: Capabilities included in a Power Profile

Feature	BPP PTx	EPP5 PTx	EPP PTx	BPP PRx	EPP PRx
A*x* or B*x* design	Yes	Yes	No	N/A	N/A
MP-A*x* or MP-B*x* design	No	No	Yes	N/A	N/A
Baseline Protocol	Yes	Yes	Yes	Yes	Yes
Extended Protocol	No	Yes	Yes	No	Yes
Authentication	N/A	Optional	Yes	N/A	Optional

2 Introduction

A Power Transmitter may damage Radio Frequency Identification (RFID) tags or Near Field Communication (NFC) cards that are in the emitting field during any phase if the emitted power levels are above the defined limit values (see Section 6, *Testing the impact of a Power Transmitter on an NFC/RFID device*, and its subsections). The highest risk of damage occurs in the *power transfer* phase, as shown in Table 4.

Table 4: Risk of damage to RFID tag or NFC card by phase

Power transfer phase	Risk of damage
Ping phase	Possible
Configuration phase	Possible
Negotiation phase	Possible
Power transfer phase	Likely

Current Foreign Object Detection (FOD) methods are not designed to detect RFID tags and NFC cards. One reason is that RFID tags and NFC cards operate at a frequency of 13.56 MHz, which is well above the frequencies used for wireless power transfer.

The goal of this informative document is to describe how RFID tags and NFC cards can be protected by extending the functionality of the Power Transmitter. In principle, two approaches can be followed.

- Integration of an NFC transceiver into the Power Transmitter. The NFC transceiver adds an extended Foreign Object Detection functionality to reliably detect RFID tags and NFC cards in Power Transmitter proximity.
- Maintaining emitted power levels of the Power Transmitter in all phases below a defined limit value. This limit is defined by specific measurement methods using the Test Proximity Integrated Circuit Card (PICC) described in Section 6, *Testing the impact of a Power Transmitter on an NFC/RFID device* (a reference card/tag). This lower power level will not damage RFID tags and NFC cards.

3 NFC/RFID card detection by a Power Transmitter

The most reliable way to detect tags is to integrate an NFC transceiver into the Power Transmitter. The NFC transceiver will use the NFC communication channel to poll for all types of tags and NFC cards. In addition, an NFC transceiver typically implements low-power tag/card detection in order to fulfill low power requirements. For this purpose, the NFC transceiver continuously monitors its antenna impedance (see Section 5, *Object detection using the NFC unit*).

The main building blocks relevant to NFC transceiver integration for tag protection are the antenna, the NFC transceiver block, and the NFC poll profile. All three points are discussed in the following subsections.

3.1 NFC antenna integration in a Power Transmitter

Due to the different operating frequencies used for power transfer and NFC communication, the Power Transmitter's Primary Coil cannot be used by the NFC interface. Accordingly, this section introduces three options for adding an NFC antenna to the Power Transmitter. All three options enable coexistence between the Primary Coil and the NFC antenna.

Selecting the appropriate design option depends partly on:

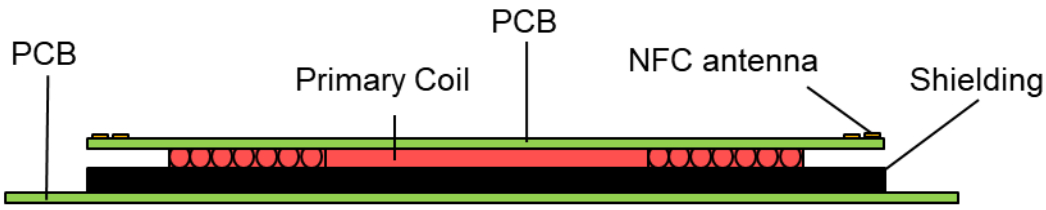
- the targeted operating volume,
- mechanical constraints, and
- space restrictions on the PCB.

3.1.1 Design option 1: NFC antenna on top of the Primary Coil

The first design option places the NFC antenna on top of the Power Transmitter's Primary Coil, as shown in Figure 2. The stack-up from the bottom to top consists of the bottom PCB, the Shielding, the Primary Coil, and the NFC antenna on the top PCB.

The NFC antenna design should achieve minimum coupling with the Primary Coil. In this case, the magnetic field generated by the Primary Coil and NFC operation have little impact on each other.

Figure 2. Example of NFC antenna on top of the Primary Coil

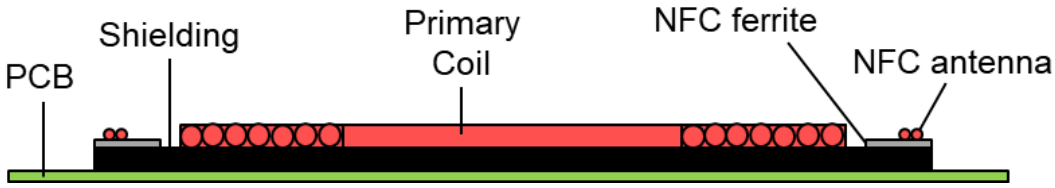


3.1.2 Design option 2: NFC antenna outside the Primary Coil

The second antenna design option places the NFC antenna on the Shielding outside the Primary Coil, as shown in Figure 3. The stack-up from the bottom to top consists of the PCB, the Shielding, and the Primary Coil. The NFC ferrite is placed on top of the Shielding outside the Primary Coil, and the NFC antenna is placed on the outer edge of the NFC ferrite.

The goal of this design is to achieve separation of the wireless power transfer and NFC operating frequencies by spatial separation and Shielding. The NFC ferrite bends the direction of the NFC field upwards and shields the NFC field from the Primary Coil. The advantage of this design is to limit construction height. However, the spatial decoupling between NFC antenna and Primary Coil might be less than in design option 1 and may require more external components for filtering via the antenna coupling circuit.

Figure 3. Example of NFC antenna outside the Primary Coil

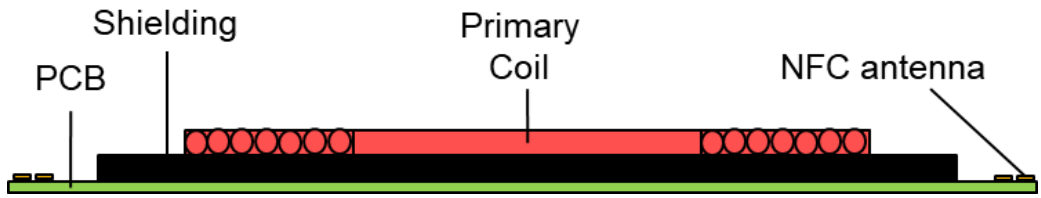


3.1.3 Design option 3: NFC antenna on mainboard PCB

The third antenna design places the NFC antenna on the PCB outside the Shielding, as shown in Figure 4. The stack-up from bottom to top consists of the PCB, the Shielding, and the Primary Coil. The NFC antenna is located well outside and below the Primary Coil. If there are metallic objects underneath the PCB, NFC ferrite can be placed underneath the NFC antenna.

In this design, the power transfer field is well shaped by the Shielding, which also provides good Shielding for the NFC antenna. The power transfer field has only a minor impact on NFC communications.

Figure 4. Example of NFC antenna on mainboard PCB



3.2 NFC transceiver integration

There is more than one way to integrate NFC transceiver functionality in a Power Transmitter. For example, the NFC transmit and receive unit can be a dedicated hardware block that manages the 13.56 MHz data exchange. The processing of NFC data and control of the NFC communication link can be executed by the Power Transmitter's Communications and Control Unit (CCU) or directly performed by an NFC unit. Both cases are introduced in more detail in the next two subsections.

From a system point of view, the CCU and NFC unit in the Power Transmitter can run independently. The only information exchange necessary is during tag detection on the Interface Surface of the Power Transmitter. In this case, a tag detection notification to the CCU is required. A detected tag should block charging and may trigger user interaction.

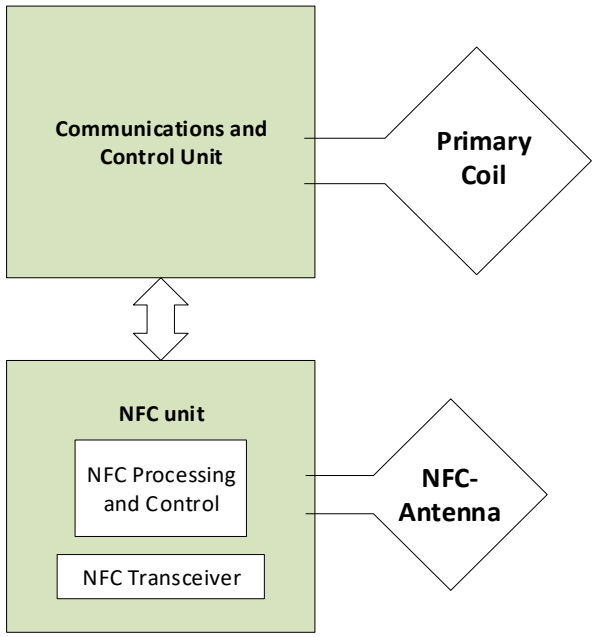
3.2.1 Using a separate NFC unit

If there are insufficient memory and processing resources available in the Communications and Control Unit, complete NFC functionality can be performed by a separate NFC unit, as shown in Figure 5. In this case, CCU and NFC functionality run independently from each other, which enables a fast and simple system integration.

An NFC unit consists of the following:

- NFC transceiver
- NFC controller
- NFC stack and tag detection applications executed by the NFC controller
- External interfaces (e.g. I/O, I2C, LEDs, etc.)

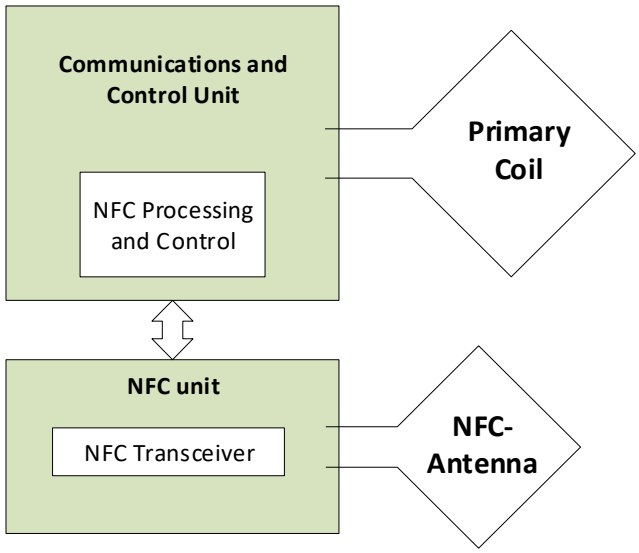
Figure 5. Independent CCU and NFC subsystems in the Power Transmitter



3.2.2 Shared NFC processing

If there are sufficient memory and processing resources available in the CCU, the NFC link can be managed in parallel. A block diagram illustrating this case is shown in Figure 6.

Figure 6. Shared Communications & Control and NFC processing



To realize a shared system, the CCU must provide 40-60 kB of flash memory depending on the complexity of the implementation. If the goal is to just detect a tag, the complexity is less than distinguishing between a tag and a mobile phone acting as a tag (i.e. *card emulation;* see Section 3.3, *NFC polling*). It is expected that the NFC stack and application integration into the Power Transmitter architecture stack is more complex compared to the independent system architecture described in Section 3.2.1, *Using a separate NFC unit*.

3.3 NFC polling

In recent decades, different communication protocols and channel encoding schemes have been defined for the 13.56 MHz Operating Frequency. To detect all different types of tags frequently seen in the field, an NFC controller should poll for all technologies. The following standards and specification provide a good overview of existing technologies operated at 13.56 MHz:

- ISO/IEC 14443 standard series
- NFC Forum Analog, Digital Protocol and Activity specifications
- ISO/IEC 18092
- ISO/IEC 15693
- ISO/IEC 18000-3 Mode 3

3.3.1 NFC polling loop in relation to power transfer phases

Tag detection should be performed for all types before and during the *ping* phase. During the *ping* phase and *power transfer phase*, the power level may be enough to damage tags. The WPC Test PICC may be used to assess whether the power level of a Power Transmitter is above the threshold to potentially damage tags. (See Section 6, *Testing the impact of a Power Transmitter on an NFC/RFID device*.)

The following actions for a Power Transmitter can be defined depending on the tag detection outcome.

- If no tag has been detected on the Power Transmitter Interface Surface, a strong charging signal is possible and the Power Transmitter can proceed to the *ping* phase.
- If a tag has been detected on the Power Transmitter Interface Surface, no strong Power Signal is allowed.

A Power Transmitter with a separate NFC unit, as described in Section 3.2.1, *Using a separate NFC unit*, should continuously poll for all tag technologies throughout all phases—even during power transfer. The polling loop cycle time should be minimized for the fastest card/tag detection (e.g. less than 50 ms).

A Power Transmitter that operates and manages the NFC link in parallel with the CCU, as described in Section 3.2.2, *Shared NFC processing*, can utilize information already obtained by the CCU in managing phase transitions. In this case, the polling for all tag technologies can be performed before the *ping* phase (see the *Qi Specification, Communications Protocol*).

The continuous polling for RFID cards and tags should be performed as an independent, parallel activity to the flow of power transfer phases described in the *Qi Specification, Communications Protocol*. If an RFID card or tag is detected, the Power Transmitter should go back to the *ping* phase and remain there until the card or tag is removed.

3.3.2 NFC Mobile Devices and tags

This section introduces different approaches to detecting tags. Additional means are provided to distinguish a tag from a mobile phone that is emulating a tag. This is required since a mobile phone with an NFC interface, or *NFC Mobile Device* (NMD), also implements a Power Receiver for wireless power transfer.

The following characteristics distinguish NFC Mobile Devices and physical tags.

3.3.2.1 NFC Mobile Devices

- NFC Forum-compliant devices must support three technologies, NFC-A, NFC-B and NFC-F, when in listen mode or in Card Emulation Mode (CEM):
  - During the RF ON period, an NMD responds to only one technology by default
- The Active Communication Mode (ACM, Active P2P) can be directly used to detect NMDs
- The NFC Forum defines CEM for: Type 3 Tag (T3T), T4AT, and T4BT Platform
- No CEM is defined for T2T, T5T (ISO/IEC 15693)

3.3.2.1.1 Tags

- NFC Forum defines the following tag types: T1T, T2T, T3T, T4AT, T4BT and T5T
  - NFC-A Technology based: T1T, T2T and T4AT
  - NFC-B Technology based: T4BT
  - NFC-F Technology based: T3T
  - NFC-V Technology based: T5T (ISO/IEC 15693)
- Physical tags only implement a single technology

An NFC unit can use the following additional information to reliably distinguish an NMD from a tag.

- The NFC unit is not expected to deal with multiple NMDs on the Power Transmitter.
- Multiple tags/cards can be detected by polling for all technologies.
- Multiple tags/cards can be detected within a single technology by collision resolution.

- Within a technology additional information is transmitted which can be used to distinguish tags from NMDs.
  - NFC-A:
    - SENS_RES/ATQA contains an indicator for a T1T (tag).
    - SEL_RES/SAK contains an indicator for T2T (tag), T4AT (tag), and NFC-DEP (NMD).
  - NFC-B:
    - No information is coded to distinguish a tag from a device.
  - NFC-F:
    - SENSF_REQ: RC-field coding to select both T3T and NMDs or T3T only.
    - SENSF_RES: NFCID2 contains an indicator for T3T (tag) or NFC-DEP (NMD).
  - NFC-V: only tags will respond to a poll command in this technology.

ACM/Active P2P: ACM is only defined for NMDs, so only NMDs will respond to the poll command.

3.3.3 NFC tag detection procedure and scenarios

This section presents a procedure to reliably distinguish a physical tag from an NMD, as well as scenarios that serve as examples.

3.3.3.1 Procedure

1. Perform technology detection to identify tags and NMDs in each technology (see the NFC Forum Activity specification).
2. Perform collision resolution to identify multiple tags or NMDs within a single technology.
3. Use protocol information (e.g. SEL_RES) of NFC-A and NFC-F technologies to distinguish tags from NMDs.
4. Use technology information to distinguish tags from NMDs. Perform a field reset and change the polling sequence.

3.3.3.2 Scenario 1: one NMD (T4AT CEM) and one T4AT tag in the field

1. Detect the technology.
   a) Poll for NFC-A: NMD and tag respond.
   b) Poll for NFC-B: no Response.
   c) Poll for NFC-F and –V: no Response.
2. Perform an NFC-A anti-collision and activation.
   a) Use information contained in SENS_RES and SEL_RES to distinguish between an NMD and a tag.
   b) If NFC-DEP support is indicated in SEL_RES, then it is an NMD.
   c) Otherwise, continue the identification process if no unique identification is possible yet.

3. Perform a reset and then detect the technology.
    a) Poll for NFC-B: 1 Response (NMD).
    b) Poll for Technologies NFC-F and -V: no Response.
    c) Poll for NFC-A: 1 Response (tag).

Conclusions:

- If an object responds to all technologies received, it is an NMD.
- If an object responds to only one technology, it is a tag.

3.3.3.3 Scenario 2: one NMD and one T4BT tag in the field

1. Perform NMD detection.
    a) Poll for NFC-A: NMD responds.
    b) Poll for NFC-B: tag responds.
    c) Poll for NFC-F and –V: no Response.
2. Perform NFC-A activation.
    a) Use the information contained in SENS_RES and SEL_RES to distinguish between an NMD and a tag.
    b) If NFC-DEP support is indicated in SEL_RES, then it is an NMD.
    c) Otherwise, continue the identification process.
3. Perform an RF reset and then a device detection.
    a) Poll for NFC-B: both NMD and tag will respond.
    b) Poll for all other technologies: no Response.
4. Perform anti-collision to check if two NMDs/tags are indeed present.
5. Perform a reset and then an NMD detection.
    a) Poll for NFC-F: NMD responds. Check SENS_RES for NFC-DEP support indication; if yes, it is an NMD.
    b) Poll for NFC-B: Tag responds.
    c) Poll for NFC-F and –V: no Response.

Conclusions:

- If an object responds to all technologies received, it is an NMD.
- If an object responds to only one technology, it is a tag.

3.3.3.4 Scenario 3: two tags in the field (one tag NFC-A and one tag NFC-B)

1. Detect the technology.
   a) Poll for NFC-A: tag responds.
   b) Poll for NFC-B: tag responds.
   c) Poll for NFC-F and –V: no Response.
2. Perform NFC-A activation.
   a) Use information contained in SENS_RES and SEL_RES to distinguish between an NMD and a tag.
   b) No indication of NFC-DEP support in SEL_RES.
3. Perform a reset and then a device detection.
   a) Poll for NFC-B: one tag Response.
   b) Poll for NFC-A: one tag Response.
   c) Poll for NFC-F and –V: no Response.
4. Perform a reset and then a device detection.
   a) Poll for NFC-F: no Response.
   b) Poll for NFC-B: one tag Response.
   c) Poll for NFC-A: one tag Response.
   d) Poll for NFC–V: no Response.

Conclusion: there are two tags in the field.

4 NFC/RFID card detection by a Power Receiver

An NFC transceiver embedded in a Power Receiver can be used to detect the presence of an RFID tag or NFC card within the power transfer operating volume. The Power Receiver can then prevent damage to the NFC card or RFID tag by stopping the Power Transfer.

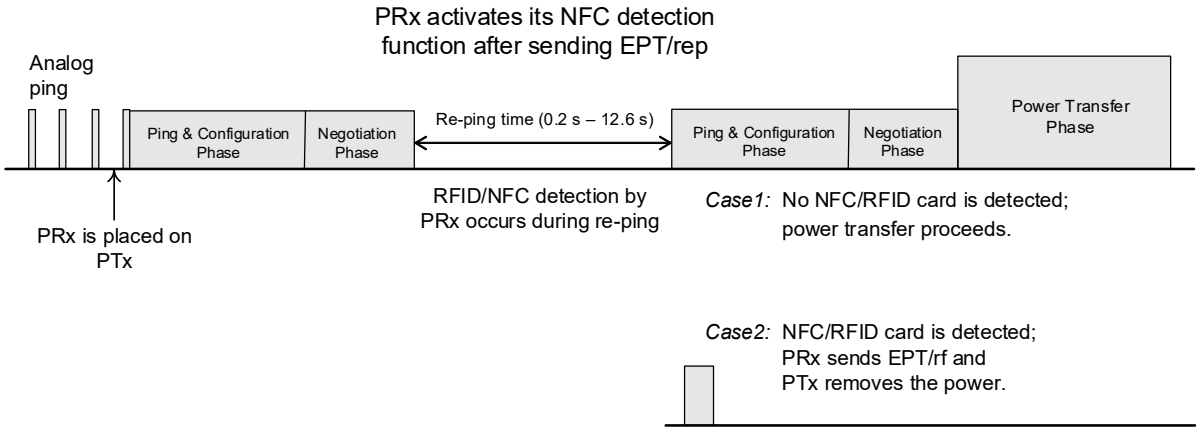
4.1 Design guidelines

Placement of the NFC transceiver in the Power Receiver is important: the NFC transceiver's operating volume should be aligned with the operating volume of the power transfer. That is, the Power Transmitter coil and NFC antenna should cover the same location.

4.2 Recommended detection procedure

To remove any interference from the power signal when detecting RFID tags and NFC cards, the Power Receiver sends an EPT/rep packet with the re-ping time packet during the negotiation phase to force the Power Transmitter to remove the power signal. During re-ping, the NFC transceiver in the Power Receiver detects the RFID tag and NFC card by applying the same technologies described in Section 3, *NFC/RFID card detection by a Power Transmitter*. A ping is executed again by the Power Transmitter after the re-ping time, and the Power Receiver sends an EPT/rf if it detects an RFID tag or NFC card. If none are detected, power transfer proceeds as defined in the Qi Specification. Figure 7 outlines this recommended procedure.

Figure 7. RFID/NFC detection by a Power Receiver



5 Object detection using the NFC unit

NFC transceivers can monitor changes in the NFC antenna's impedance. These impedance changes can be caused by placing either metallic objects or inductive coupled objects, such as RFID tags or NFC cards, on the antenna.

Antenna impedance monitoring operates with very low power consumption—typically less than 100µA average current—and can be used for low-power object detection in transmitter standby mode.

5.1 Low power object detection in standby

The NFC unit is set up to periodically check (e.g. every 300ms) the NFC antenna impedance.

- If no impedance change is detected or the impedance is within a defined window, the NFC unit enters standby mode and waits a configurable time before starting the next detection process.
- If an NFC impedance change is detected or the impedance is outside a defined range, the NFC unit wakes up and performs the NFC tag detection procedure.
- If a physical RFID tag or NFC card is detected, the NFC unit should notify the Power Transmitter and may also provide a user notification to remove the RFID tag or NFC card.
- If no physical RFID tag or NFC card is detected, the NFC transceiver can signal to the Power Transmitter (e.g. via interrupt line or any other interface) to start a Power Receiver detection cycle.

5.2 Low power object detection in the power transfer phase

The NFC unit is set up to periodically check (e.g. every 50ms) the NFC antenna impedance during the *power transfer* phase. If no impedance change is detected or the impedance is within a defined range, the NFC unit enters standby mode and waits a configurable time before starting the next detection process.

If an NFC antenna impedance change is detected or the impedance is outside a defined range, the NFC unit wakes up and performs the RFID detection process. If no physical RFID tag or NFC card is detected, the NFC unit can signal to the Power Transmitter that it has detected a load change without any RFID tag or NFC card present. The Power Transmitter may use this information for further actions, e.g. performing additional FOD methods.

Alternatively, the Power Transmitter may actively trigger the NFC antenna impedance check via any digital interface to perform an additional FOD method.

6 Testing the impact of a Power Transmitter on an NFC/RFID device

NFC standards are defining test methods for NFC transmitters to check that their field emission levels do not exceed specified limits. Tags and cards are tested to avoid being damaged.

The NFC unit field emission test is based on a specific test Proximity Integrated Circuit Card (PICC). The WPC Test PICC transforms the NFC field level into a simple DC voltage level. The coil design parameters of the WPC Test PICC have been selected to represent an NFC/RFID card coupling to a Power Transmitter. A Power Transmitter Product that fails this test can either implement a method to solve the risk of damage as described in Section 3, *NFC/RFID card detection by a Power Transmitter*, or rely on detection by the Power Receiver as described in Section 4, *NFC/RFID card detection by a Power Receiver*.

6.1 WPC Test PICC dimensions

The design of the WPC Test PICC is similar to the Reference PICC 3 defined in ISO/IEC 10373-6 with modified coil parameters.

The NFC antenna dimensions of the WPC Test PICC are as follows:

- Square outline, 40 mm x 40 mm for better coupling
- Track width, 0.5 mm (same as ISO Reference PICCs)
- Track spacing, 0.5 mm (same as ISO Reference PICCs)
- Number of turns: 8
- Self-inductance: (4.1 ± 10%) µH

6.2 Construction of the WPC Test PICC

The WPC Test PICC shall have a circuit diagram as defined in Figure 8 and component values as defined in Table 5. The WPC Test PICC coil layouts are defined in Figure 9. If connectors are used between the coils and the circuitry, those connectors shall have minimal, if any, effect on the RF measurements.

Figure 8. WPC Test PICC circuit diagram

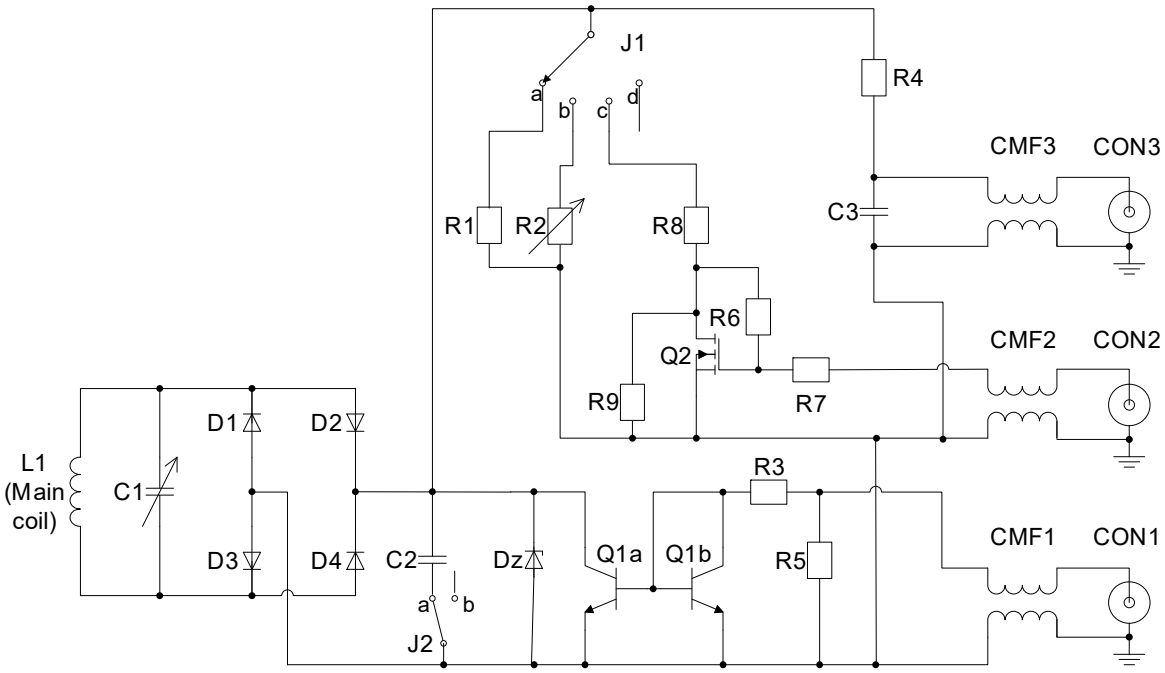


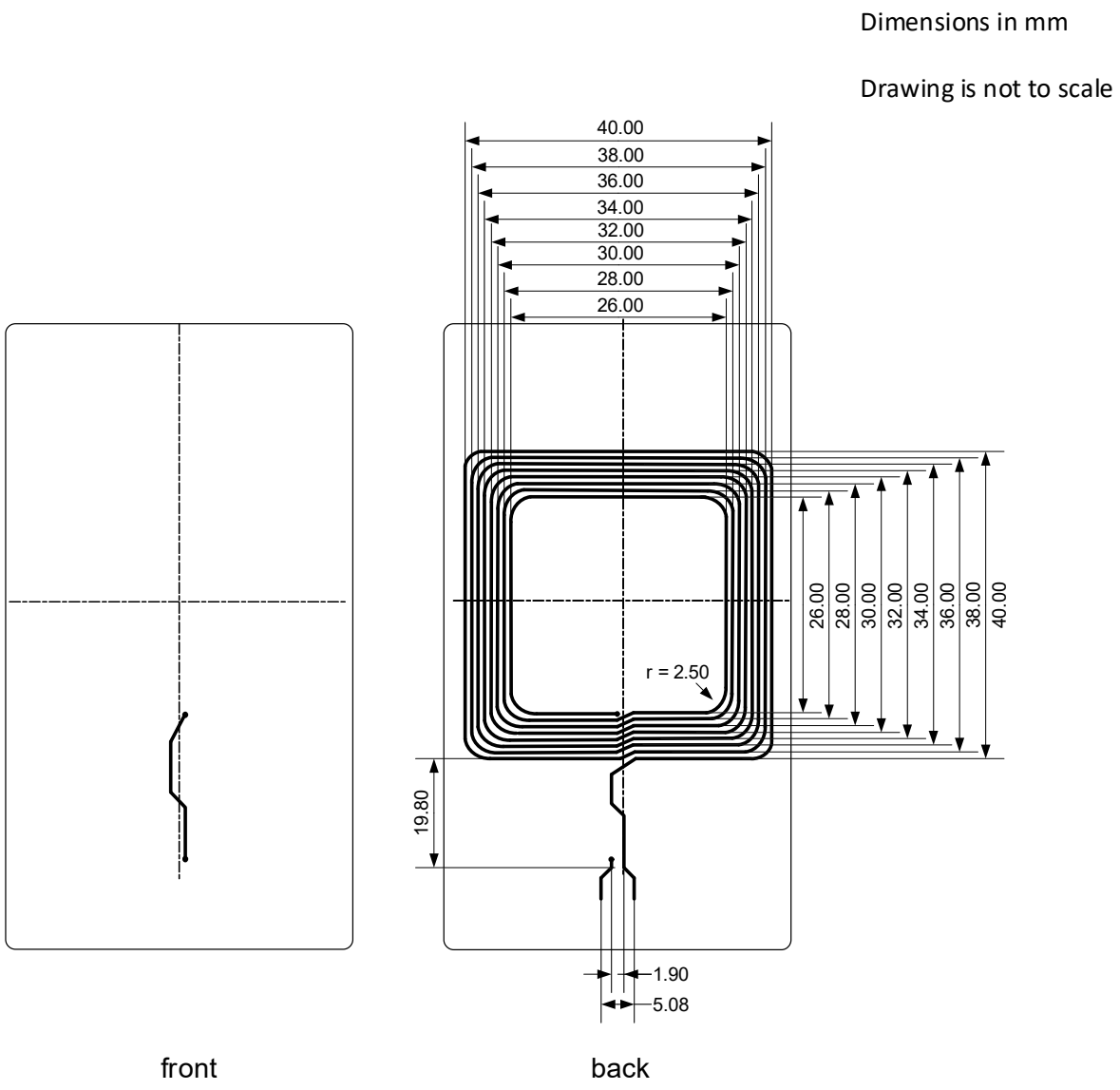
Table 5: WPC Test PICC components list

Component	Value	Component	Value
L1		C1	3 pF – 10 pF [a]
R1	1.8 kΩ	C2	27 pF
R2	0 kΩ – 2 kΩ [a]	C3	1 nF
R3	220 Ω	D1, D2, D3, D4	BAR43S or equivalent
R4	51 kΩ	Dz	BZV55C27, 27 V or equivalent[b]
R5	51 Ω	Q1a, Q1b	BCV61A or equivalent
R6	500 kΩ	Q2	BSS83 or equivalent
R7	110 kΩ	CMF1, CMF2, CMF3	ACM3225 -102-2P or equivalent
R8	51 Ω	CON1, CON2, CON3	RF connector
R9	1.5 kΩ		

[a] A multi-turn potentiometer (turns ≥ 10) should be used.

[b] Care should be taken with the junction capacitance, package capacitance, series inductance, and series resistance of equivalent diodes. Note that these values may not be available in the component's datasheet.

Figure 9. WPC Test PICC main coil layouts



The coil's track width and spacing shall each be 0.5 mm with a relative tolerance of ±20%.

Printed circuit board (PCB): FR4 material, thickness 0.76 mm with a relative tolerance of ±10%, double-sided with 35 µm copper.

6.3 WPC Test PICC calibration

The calibration procedure as defined in ISO/IEC 10373-6:2016, 6.1.1.2 shall be performed with following modifications.

- In step a): Replace “19 MHz” with “13.56 MHz” and replace “Reference PICC” with “WPC Test PICC.”
- In step b): The Hmax as defined for Class 3 PICCs (Hmax = 8.5A/m(rms)) shall be used. According to ISO/IEC 14443-1:2016, 4.4 the calibrated field strength consequently corresponds to 4/3 times Hmax (4/3 * 8.5 A/m(rms)) equivalent to 11.3A/m(rms).
- After step c): Ignore the warning.

6.4 Test procedure using the WPC Test PICC

The test procedure should include using the WPC Test PICC to test the Analog and Digital Ping levels. If the ping levels are below the limit value of 3 VDC, RFID cards and tags are protected during the ping phases.

The test procedure should include the testing of the power transfer levels with the WPC Test PICC. If the level during power transfer in Power Receiver offset position does not exceed the limit value of 3 V DC, RFID cards and tags are protected during power transfer.

6.4.1 Test for Analog & Digital Ping

1. Place the WPC Test PICC on a Power Transmitter Product in a way that its antenna is center-aligned with the Power Transmitter Product’s coil. Leave it there for 20 seconds.
2. Monitor (using a scope) and note the maximum (peak) voltage at the WPC Test PICC V_{out} during analog and Digital Ping.

If the measured voltage exceeds 3 V, the test fails.

6.4.2 Test for power transfer

1. Place the WPC Test PICC on a Power Transmitter Product in a way that its antenna is center-aligned with the Power Transmitter Product’s coil.
2. Place TPR#1A on top of the WPC Test PICC in a way that its coil center is off-aligned from the center of the Power Transmitter Product’s coil. This will maximize the voltage at the WPC Test PICC V_{out}.
3. Monitor (using a scope) and note the maximum (peak) Voltage at the WPC Test PICC V_{out}.
4. If the Power Transmitter Product is an EPP Power Transmitter, repeat steps 2 and 3 with TPR#MP1B.

If the measured voltage exceeds 3 V, the test fails.