IEC 63563-8

Edition 1.0 2025-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Qi Specification version 2.0 –
Part 8: NFC Tag Protection

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, …). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

IEC 63563-8

Edition 1.0 2025-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Qi Specification version 2.0 –
Part 8: NFC Tag Protection**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

QI SPECIFICATION VERSION 2.0 –

Part 8: NFC Tag Protection

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.

2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.

3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.

5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.

6) All users should ensure that they have the latest edition of this publication.

7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.

8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 63563-8 has been prepared by technical area 15: Wireless Power Transfer, of IEC technical committee 100: Audio, video and multimedia systems and equipment. It is an International Standard.

It is based on *Qi Specification version 2.0, NFC Tag Protection* and was submitted as a Fast-Track document.

The text of this International Standard is based on the following documents:

Draft	Report on voting
100/4252/FDIS	100/4283/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

The structure and editorial rules used in this publication reflect the practice of the organization which submitted it.

This document was developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

WIRELESS POWER

CONSORTIUM

Qi Specification

NFC Tag Protection

Version 2.0

April 2023

DISCLAIMER

RELEASE HISTORY

Specification Version	Release Date	Description
2.0	April 2023	Initial release of the v2.0 Qi Specification.

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 Tag Protection
- Authentication Protocol

1.2 Scope

The *Qi Specification, NFC/RFID Card Protection* (this document) provides guidelines 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.

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)							
B_1			16-bit Numeric Data Field					(lsb)
B_2		Other Field			(msb)			
B_3	10-bit Numeric Data Field					(lsb)		Field

Figure 1. Examples of fields in a data packet

16-bit Numeric Data Field

b_{15} b_{14} b_{13} b_{12} b_{11} b_{10} b_9 b_8	b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0
B_0	B_1

10-bit Numeric Data Field

	b_9 b_8 b_7	b_6 b_5 b_4 b_3 b_2 b_1 b_0	
B_2		B_3	
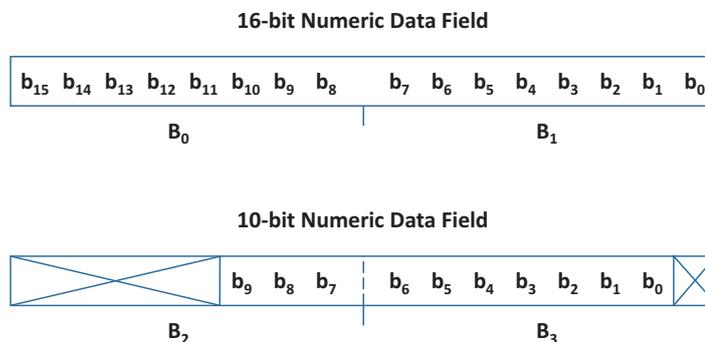
1.5.4 Notation of text strings

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. $P_{\mathrm{L}}^{(\mathrm{pot})}$ = 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 can damage Near Field Communication (NFC) tags present in the Operating Volume during any phase if the emitted power levels are above the defined limit values (see Section 2, *Introduction*, and its subsections).

For more information about NFC tags, see https://nfc-forum.org/.

The highest risk of damage occurs in the *power transfer* phase, as shown in Table 4.

Table 4: Risk of damage to NFC tags by protocol phase

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

2.1 NFC tag detection and protection

The goal of this document is to describe how NFC tags can be detected and protected by extending the functionality of the Power Transmitter Product or Power Receiver Product.

2.1.1 NFC tag detection

By integrating an NFC transceiver into a Power Transmitter Product or into a Power Receiver Product, any NFC tag that can be present between the Power Transmitter Product and the Power Receiver Product can be reliably detected. The capabilities of the devices determines which one will execute NFC tag detection.

- If neither the Power Transmitter Product nor the Power Receiver Product can detect NFC tags, NFC tag protection does not happen and any NFC tag in the Operating Volume are susceptible to damage.

- If either the Power Transmitter Product or the Power Receiver Product (but not both) can detect NFC tags, that device should execute tag detection.

- If both the Power Transmitter Product and the Power Receiver Product can detect NFC tags, one or both of the devices should execute tag detection.

Selection of the device that should execute NFC tag detection happens when the Power Transmitter and Power Receiver exchange information in the negotiation phase.

See Section 3, *NFC tag protection and device communication*, for further information.

2.1.2 Protecting NFC tags

A Power Transmitter can protect NFC tags by maintaining the magnetic field levels in all phases of the power transfer protocol below a defined limit value. This limit is defined by specific measurement methods using the Test Proximity Integrated Circuit Card (PICC) described in Section 7, *Testing the impact of a Power Transmitter Product on an NFC tag*, and helps to ensure that NFC tags are not damaged.

> **NOTE:** In rare cases, damage can still occur even at magnetic field levels below the limit value.

3 NFC tag protection and device communication

A Power Receiver should send a GRQ/xcap data packet to an EPP Power Transmitter during the negotiation phase to examine the Power Transmitter Product's extended capabilities. The XCAP data packet returned in response provides the result of any NFC tag detection operation it has executed. See Section 9.5, *Qi Specification, Communications Protocol*, for more information.

The Power Receiver Product should perform one of the actions listed in Table 5 depending on values contained in the TPS, TPE, and TDS fields of the XCAP data packet.

Table 5: Power Receiver actions based on XCAP data

XCAP data	XCAP meaning	Power Receiver Product action
TPS = ZERO	The Power Transmitter Product does not support NFC tag detection.	The Power Receiver Product should perform NFC tag detection as defined in Section 5, *NFC tag detection by a Power Receiver Product*.
TPS = ONE TDE = ONE TDS = 0	The Power Transmitter Product supports NFC tag detection and has not detected a tag.	The power transfer proceeds as defined in the *Qi Specification, Communications Protocol*.
TPS = ONE TDE = ZERO TDS = 0	The Power Transmitter Product supports NFC tag protection but has not executed the latter.	To proceed, the Power Receiver Product should select one of the following actions: ▪ Send an EPT/rep data packet and perform tag detection itself as defined in Section 5, *NFC tag detection by a Power Receiver Product* ▪ Send an EPT/ptxnfc data packet to request the Power Transmitter Product to perform tag detection. This should cause the Power Transmitter Product to remove its Power Signal and perform NFC tag detection.
TPS = ONE TDE = ONE TDS = 1	The Power Transmitter Product supports NFC tag protection and has detected a single tag. NOTE: The Power Transmitter Product may not be able to distinguish between an NFC tag and the NFC interface of the Power Receiver Product.	The Power Receiver Product should select one of the following actions to proceed: ▪ Send an EPT/rep data packet itself as defined in Section 5, *NFC tag detection by a Power Receiver Product*. ▪ Send an EPT/ptxnfc data packet to request the Power Transmitter to perform tag detection. This should cause the Power Transmitter Product to remove its Power Signal and perform NFC tag detection. ▪ Proceed to the power transfer phase and limit its drawing the power level to 5 W. ▪ Proceed at full power if it knows that its own NFC transceiver is active in the Operating Volume. ▪ Send an EPT/nfc data packet and power transfer terminates. **Note:** Whenever an NFC tag is potentially in the Operating Volume, the Power Receiver Product should provide a warning to the user.

Table 5: Power Receiver actions based on XCAP data (Continued)

XCAP data	XCAP meaning	Power Receiver Product action
TPS = ONE TDE = ZERO TDS = 2	The Power Transmitter Product supports NFC tag protection and has detected multiple tags. NOTE: TDS=2 may be multiple NFC tags or a tag and an NMD.	The Power Receiver Product should select one of the following actions to proceed: ▪ Send an EPT/rep data packet itself as defined in Section 5, *NFC tag detection by a Power Receiver Product*. ▪ Send an EPT/ptxnfc data packet to request the Power Transmitter to perform tag detection. This should cause the Power Transmitter Product to remove its Power Signal and perform NFC tag detection. ▪ Proceed to the power transfer phase and limit its drawing the power level to 5 W. ▪ Proceed at full power if it knows that its own NFC transceiver is active in the Operating Volume. ▪ Send an EPT/nfc data packet and power transfer terminates. Whenever an NFC tag is potentially in the Operating Volume, the Power Receiver Product should provide a warning to the user.

The following generic guidelines apply to EPP Power Transmitter Products for NFC tag detection.

The Power Transmitter Product does not detect NFC tags

If the Power Transmitter Product does not detect any NFC tag (TDS is 0 in the XCAP data packet), it should proceed with normal operation.

The Power Transmitter Product detects one NFC tag

When a Power Receiver Product requests an XCAP data packet, it indicates to the Power Transmitter that it supports NFC tag protection. The Power Transmitter should not limit the Negotiable Load Power when it detects an NFC tag.

If a Power Receiver Product does not request an XCAP data packet, the Power Transmitter may assume that the it does not support NFC tag protection. In that case, the Power Transmitter should limit the Negotiable Load Power to 5 W or below to avoid damaging the detected NFC tag.

The Power Transmitter Product detects more than one NFC tag

The Power Transmitter should limit the Negotiable Load Power to 5 W or below. The Power Receiver Product cannot proceed at full power.

4 NFC tag detection by a Power Transmitter Product

The most reliable way to detect NFC tags in the Operating Volume is to integrate an NFC transceiver into the Power Transmitter Product. The transceiver uses the NFC communication channel to poll for all types of NFC tags.

In addition, an NFC transceiver typically implements low-power tag detection in order to fulfill low power requirements. For this purpose, the NFC transceiver continuously monitors its antenna impedance (see Section 6, *Tag 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.

4.1 NFC antenna integration in a Power Transmitter Product

Due to the different operating frequencies used for power transfer and NFC communication, the Power Transmitter Product'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 Product. 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.

4.1.1 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 Product'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
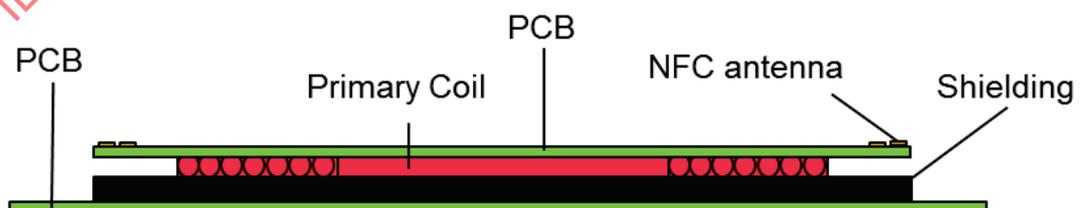
4.1.2 Design option 2: NFC antenna outside the Primary Coil

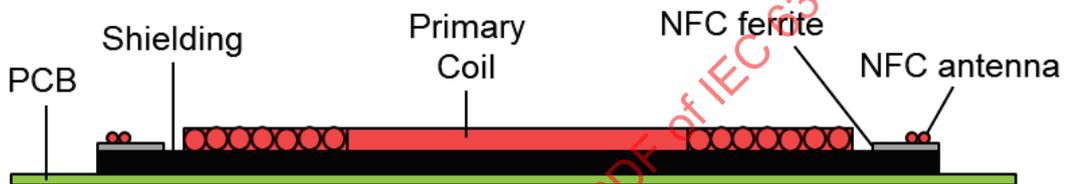The second antenna design option places the NFC antenna on the Shielding outside the Primary Coil, as shown in Figure 3. The stack-up from the bottom to top consists of the PCB, the Shielding, and the Primary Coil. The NFC ferrite is placed on top of the Shielding outside the Primary Coil, and the NFC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

4.1.3 Design option 3: NFC antenna on the main board 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 the main board PCB
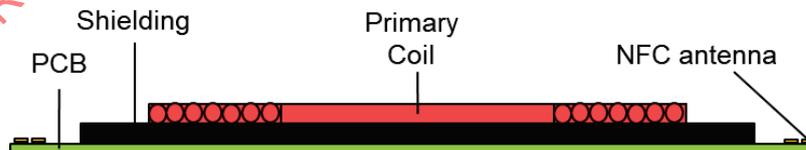
4.2 NFC transceiver integration

There is more than one way to integrate NFC transceiver functionality in a Power Transmitter Product. 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 Product can run independently. The only information exchange necessary is during tag detection on the Interface Surface of the Power Transmitter Product. In this case, a tag detection notification to the CCU is required. A detected tag should block charging and may trigger user interaction.

4.2.1 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
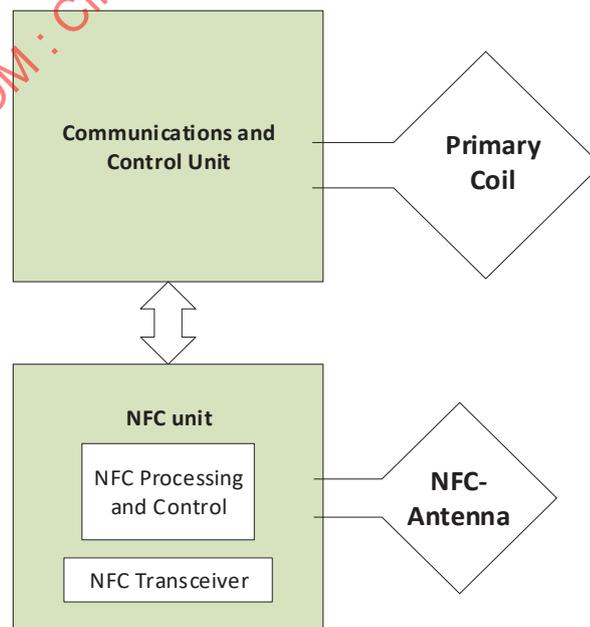
4.2.2 Shared NFC processing

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
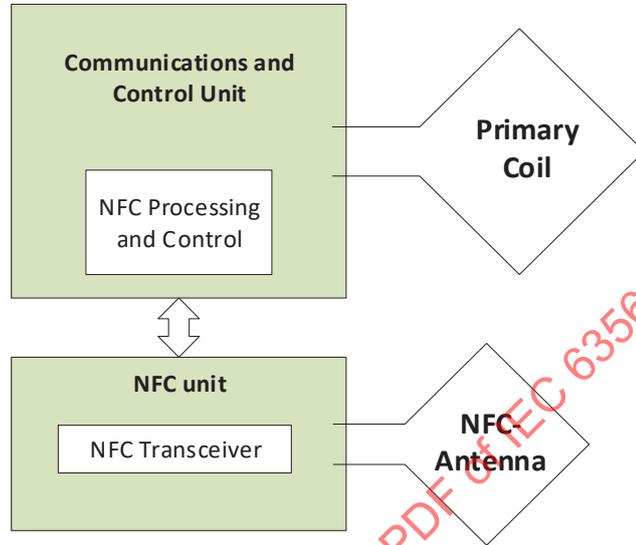
To realize a shared system, the CCU must provide 40-60 kB of flash memory depending on the complexity of the implementation. If the goal is to just detect a tag, the complexity is less than distinguishing between a tag and a mobile phone acting as a tag (i.e. *tag emulation;* see Section 4.3, *NFC polling*). 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 4.2.1, *Using a separate NFC unit.*

4.3   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

4.3.1   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 7, *Testing the impact of a Power Transmitter Product on an NFC tag*.)

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 4.2.1, *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 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 4.2.2, *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 NFC 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 NFC tag is detected, the Power Transmitter should go back to the *ping* phase and remain there until the tag is removed.

4.3.2 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.

4.3.2.1 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

4.3.2.1.1 Tags

- NFC Forum defines the following tag types: T1T, T2T, T3T, T4AT, T4BT and T5T
  - NFC-A Technology based: T1T, T2T and T4AT (ISO/IEC 14443)
  - NFC-B Technology based: T4BT (ISO/IEC 14443)
  - NFC-F Technology based: T3T
  - NFC-V Technology based: T5T
- 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.

4.3.3 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.

4.3.3.1 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.

4.3.3.2 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.

4.3.3.3 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.

4.3.3.4 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.

5 NFC tag detection by a Power Receiver Product

An NFC transceiver embedded in a Power Receiver Product can be used to detect the presence of an NFC tag within the power transfer Operating Volume. The Power Receiver Product can then prevent damage to the NFC tag by stopping the Power Transfer.

5.1 Design guidelines

Placement of the NFC transceiver in the Power Receiver Product 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.

5.2 Recommended detection procedure

To remove any interference from the power signal when detecting NFC tags, the Power Receiver Product sends an EPT/rep data 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 Product detects the tag by applying the same technologies described in Section 4, *NFC tag detection by a Power Transmitter Product*. A ping is executed again by the Power Transmitter after the re-ping time, and the Power Receiver sends an EPT/nfc if it detects an NFC tag. If none are detected, power transfer proceeds as defined in the *Qi Specification*.

Figure 7 outlines this recommended procedure.

Figure 7. NFC tag detection by a Power Receiver Product