SLOVENSKI STANDARD
oSIST prEN IEC 63563-9:2024

01-julij-2024

Različica specifikacije Qi 2.0 - 2.del: Avtentikacijski protokol (Hitri postopek)

Qi specification version 2.0 - Part 9: Authentication protocol (Fast track)

Ta slovenski standard je istoveten z: **prEN IEC 63563-9:2024**

ICS:

29.240.99	Druga oprema v zvezi z omrežji za prenos in distribucijo električne energije	Other equipment related to power transmission and distribution networks
33.160.99	Druga avdio, video in avdiovizuelna oprema	Other audio, video and audiovisual equipment
35.200	Vmesniška in povezovalna oprema	Interface and interconnection equipment

oSIST prEN IEC 63563-9:2024 **en,fr,de**

100/4130/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 63563-9 ED1**	
DATE OF CIRCULATION: **2024-05-03**	CLOSING DATE FOR VOTING: **2024-07-26**
SUPERSEDES DOCUMENTS:	

IEC TA 15 : WIRELESS POWER TRANSFER	
SECRETARIAT: Korea, Republic of	SECRETARY: Mr Ockwoo Nam
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 106,TC 108	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	
☐ SUBMITTED FOR CENELEC PARALLEL VOTING	☒ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant “In Some Countries” clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (SEE AC/22/2007 OR NEW GUIDANCE DOC).

TITLE:

Qi Specification version 2.0 - Part 9: Authentication Protocol (Fast track)

PROPOSED STABILITY DATE: 2029

NOTE FROM TC/SC OFFICERS:

This document is only in PDF format. IEC and WPC agreed to use the pdf files as this is an adoption.

WIRELESS POWER CONSORTIUM

Qi Specification

Authentication Protocol

Version 2.0

April 2023

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
v2.0	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

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, Authentication Protocol* (this document) defines the architecture and application-level messaging for the Authentication of a Power Transmitter Product by a Power Receiver to ensure that the Power Transmitter Product is both Qi certified and the product of a registered manufacturer.

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.

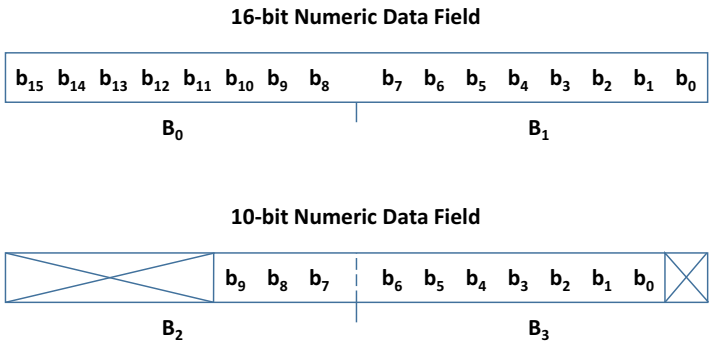
1.5.3 Fields in a data packet

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 Overview

The *Qi Specification, Authentication Protocol* (this document) defines a protocol for a Power Receiver to authenticate a Power Transmitter. In this context, Authentication is a tamper-resistant method to establish and verify the identity of the Power Transmitter, enabling the Power Receiver to trust the Power Transmitter to operate within the bounds of the *Qi Specification*. This Authentication protocol version 1.0 makes use of Data Transport Streams between the Power Receiver and Power Transmitter as defined in the *Qi Specification, Communications Protocol*.

Authentication allows an organization to set and enforce a policy with regard to acceptable products. This will permit useful security assurances in real world situations. For example, a mobile phone manufacturer concerned about product damage or safety hazards resulting from substandard wireless charging devices can set a policy limiting the power drawn from an untrusted wireless charger.

This document aims to be closely aligned with the USB Authentication specification, particularly as it is likely that products will exist in the market that support both.

In addition to this document, the *WPC Manufacturer Agreement* covers legal and implementation requirements, including secure storage and handling of secrets (Annex A) and revocation rules and procedure (Annex B). For further information or to obtain a copy of this agreement, contact: info@wirelesspowerconsortium.com.

2.1 References

Unless specified otherwise, all standards specified, including those from ISO, ITU, and NIST refer to the version or edition which is more recent, as of 1 January 2018.

ECDSA

- ANSI X9.62-2005; Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA) (available at www.global.ihs.com or https://www.techstreet.com)
- NIST-FIPS-186-4, Digital Signature Standard (DSS), Section 6, Federal Information Processing Standards Publication, July 2013 (available at: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf)
- ISO/IEC 14888-3 Digital signatures with appendix—Part 3: Discrete logarithm based mechanisms (Clause 6.6)

NIST P-256, secp-256r1

- NIST-FIPS-186-4, Digital Signature Standard (DSS), Appendix D: Recommended Elliptic Curves for Federal Government Use, Federal Information Processing Standards Publication, July 2013 (available at: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf)
- ISO/IEC 15946 Cryptographic techniques based on elliptic curves (NIST P-256 is included as example)

NOTE: The ISO/IEC 15946 series treats elliptic curves differently from FIPS 186- 4. ISO/IEC 15946-5 is about elliptic curve generation. That is, based on the method in part 5, each application and implementation can generate its own curves to use. In other words, there are no ISO/IEC recommended curves. P-256 is considered an example in ISO/IEC 15946. In addition, Elliptic Curve signatures and key establishment schemes have been moved to ISO/IEC 14888 and ISO/IEC 11770 respectively, together with other discrete-log based mechanisms. Test vectors (examples) using P-256 are included for each of those mechanisms.

SEC 1

- Certicom Corp., Standards for Efficient Cryptography Group (SECG), SEC 1: "Elliptic Curve Cryptography," Version 1.0, September 2000 (available at: https://www.secg.org/SEC1-Ver-1.0.pdf)

SEC 2

- Certicom Corp., Standards for Efficient Cryptography Group (SECG), SEC 2: "Recommended Elliptic Curve Domain Parameters," Version 2.0, January 2010 (available at: http://www.secg.org/sec2-v2.pdf)