SLOVENSKI STANDARD
oSIST prEN IEC 63758-11:2026

01-november-2026

Specifikacija Qi - Različica 2.3 - 11.del: Avtentikacijski protokol (hitri postopek)

Qi Specification - Version 2.3 - Part 11: Authentication protocol (Fast Track)

Sample Document

Ta slovenski standard je istoveten z: **prEN IEC 63758-11:2026**

---

get full document from standards.iteh.ai

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 63758-11:2026 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

Sample Document

get full document from standards.iteh.ai

100/4554/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 63758-11 ED1**	
DATE OF CIRCULATION: **2026-09-18**	CLOSING DATE FOR VOTING: **2026-12-11**
SUPERSEDES DOCUMENTS:	

IEC TC 100 : AUDIO, VIDEO AND MULTIMEDIA SYSTEMS AND EQUIPMENT	
SECRETARIAT: Japan	SECRETARY: Ms Mahiru Uehara
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 106,TC 108	HORIZONTAL FUNCTION(S):
ASPECTS CONCERNED:	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

Attention IEC-CENELEC parallel voting

The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting.

The CENELEC members are invited to vote through the CENELEC online voting system.

Sample Document
Use full document from standards.iteh.ai

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 2.3 - Part 11: Authentication protocol (Fast Track)

PROPOSED STABILITY DATE: 2029

NOTE FROM TC/SC OFFICERS:

As this is a fast-track process offered by WPC, the Word file is not provided.

Copyright © 2026 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

oSIST prEN IEC 63758-11:2026

WIRELESS POWER

CONSORTIUM

Qi Specification

Authentication Protocol

Sample Document

get full document from standards.iteh.ai

Version 2.3

Publish Date: 08 December 2025

oSIST prEN IEC 63758-11:2026 • https://standards.iteh.ai/catalog/standards/sist/4b0a6606-8838-40e1-aa3a-c0f2a60835b7/osist-pren-iec-63758-11-2026

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.

Sample Document

get full document from standards.iteh.ai

Contents

1. General 6

1.1 Structure of the Qi Specification 6
1.2 Scope 7
1.3 Compliance 7
1.4 References 7
1.5 Conventions 8
1.5.1 Notation of numbers 8
1.5.2 Tolerances 8
1.5.3 Fields in a data packet 8
1.5.4 Notation of text strings 9
1.5.5 Short-hand notation for data packets 9

2. Overview 10

2.1 References 10
2.1.1 ECDSA 10
2.1.2 NIST P-256, secp-256r1 10
2.1.3 SEC 1 10
2.1.4 SEC 2 11
2.1.5 SHA-256 11
2.1.6 SP800-90A 11
2.1.7 SP800-90B 11
2.1.8 USB Authentication 11
2.1.9 X.509 11
2.2 Cryptographic methods 11
2.2.1 Random number generators 11
2.3 Security overview 11
2.3.1 Methodology 12
2.3.2 Periodic re-Authentication 12
2.4 Impact to existing ecosystem 12
2.5 Support for revocation 12

3. Certificates and private keys 13

3.1 Certificate Chains 13
3.2 Certificates 14
3.2.1 Format of Certificates 14
3.3 Certificate Chain slots 25
3.3.1 Provisioning 26
3.4 Power Transmitter private keys 26
3.5 Other private keys 26

4. Authentication protocol 27

4.1 Digest query 27

Sample Document
Get full document from standards.iteh.ai

4.2 Certificate Chain read 27
4.3 Authentication challenge 27
4.4 Errors and alerts 27
4.4.1 Invalid request 27
4.4.2 Unsupported protocol version 28
4.4.3 Busy 28
4.4.4 Unspecified 28
5. Authentication messages 29
5.1 Authentication message header 29
5.2 Authentication requests 29
5.2.1 GET_DIGESTS 30
5.2.2 GET_CERTIFICATE 31
5.2.3 CHALLENGE 32
5.3 Authentication responses 32
5.3.1 DIGESTS 32
5.3.2 CERTIFICATE 34
5.3.3 CHALLENGE_AUTH 35
5.3.4 Error 37
6. Timing requirements 39
6.1 Power Receiver timing requirements 39
6.2 Power Transmitter timing requirements 39
7. Protocol flow examples 41
7.1 Simple flow 42
7.2 Flow with caching 43
7.3 Flow with caching and revocation 44
7.4 Challenge first flow 45
8. Cryptographic examples (informative) 47
8.1 X.509 Certificate basics 47
8.1.1 Verifying the ECDSA signature of an X.509 Certificate 47
8.2 Dummy Root CA Certificate 48
8.2.1 Dummy Root CA Certificate – DER-encoded 48
8.2.2 Dummy Root CA Certificate – hash 48
8.2.3 Dummy Root CA Certificate – data 49
8.2.4 Verification of the Root CA Certificate signature 49
8.3 Manufacturer CA Certificate Example 50
8.3.1 Example Manufacturer CA Certificate — DER-encoded 52
8.3.2 Example Manufacturer CA Certificate - data 52
8.3.3 Verification of the Manufacturer CA Certificate signature 53
8.4 Example Product Unit Certificates 53
8.4.1 Example 1: maximum length Product Unit Certificate 53
8.4.2 Example 2: typical length Product Unit Certificate 55

Sample Document
get full document from standards.iteh.ai

8.5 Certificate Chain and digest of certificates example 57
8.5.1 Example 1: maximum length Certificate Chain 57
8.5.2 Example 2: typical length Certificate Chain 59
8.6 Authentication examples 59
8.6.1 Test of example 1, maximum length Certificate Chain 59
8.6.2 Test of example 2, typical length Certificate Chain 68
Annex A: Sample data 78
A.1 Dummy Root CA Certificate in PEM format 78
A.2 Dummy Root CA Certificate in ASN.1 parser output 79
A.3 Manufacturer CA Certificate in PEM Format 80
A.4 Manufacturer CA Certificate in ASN.1 parser output 81
A.5 Product Unit Certificate, example 1 in PEM format 82
A.6 Product Unit Certificate, example 1 in ASN.1 parser output 83
A.7 Product Unit Certificate, example 2 in PEM format 84
A.8 Product Unit Certificate, example 2 in ASN.1 parser output 85
Annex B: Behaviour Guidelines for Qi PRx when a PTx Fails to Authenticate 86
B.1 BPP Power Transmitter Products 86
B.2 Legacy EPP Power Transmitter Products 86
B.3 EPP5 Power Transmitter Products 86
B.4 Authentication failure with Power Transmitter Products 86
B.4.1 Incorrect product unit certificate 86
Annex C: Object Identifiers (OID) 87

Sample Document
get full document from standards.iteh.ai

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. An important application area comprises flat-surface devices such as mobile phones and chargers operating at power levels up to 25 W.

1.1 Structure of the Qi Specification

General documents

- Introduction
- Glossary, Acronyms, and Symbols
- Technical System Overview
- Power Profiles

System description documents

- Mechanical, Thermal, and User Interface
- Power Delivery
- Communications Physical Layer
- Communications Protocol
- Foreign Object Detection
- NFC Tag Protection
- Authentication Protocol
- MPP Communications Protocol
- MPP Magnetics Design
- MPP Power Delivery
- MPP Communications Physical Layer
- MPP Foreign Object Detection
- MPP Design Guidelines (Informative)
- Magnetic Covers
- Active Alignment System
- Thermal Management Protocol

Sample Document
get full document from standards.iteh.ai

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.

Sample Document
get full document from standards.iteh.ai

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 (table)

Sample Document
get full document from standards.iteh.ai

	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	16-bit Numeric Data Field						(lsb)	Field

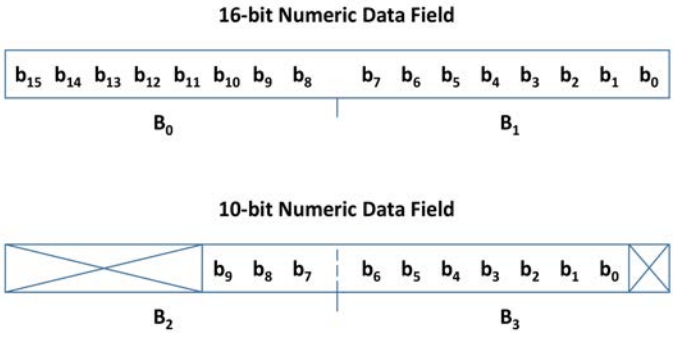


Figure 1 - Examples of fields in a data packet

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.

Sample Document

get full document from standards.iteh.ai

oSIST prEN IEC 63758-11:2026

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 (*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.

Sample Document
get full document from standards.iteh.ai

2.1.1 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)

2.1.2 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.

2.1.3 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)

oSIST prEN IEC 63758-11:2026 • https://standards.iteh.ai/catalog/standards/sist/4b0a6606-8838-40e1-aa3a-c0f2a60835b7/osist-pren-iec-63758-11-2026

2.1.4 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)

2.1.5 SHA-256

- NIST-FIPS-180-4 (available at: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf)
- ISO/IEC 10118-3 Hash-functions—Part 3: Dedicated hash-functions (Clause 10)

2.1.6 SP800-90A

- NIST-SP-800-90A Revision 1 (available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf.)

2.1.7 SP800-90B

- NIST-SP-800-90B (available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf)

2.1.8 USB Authentication

- Universal Serial Bus Type-C™ Authentication Specification (available at http://www.usb.org/developers/docs/ as part of the USB 3.2 Specification download package)

Sample Document

2.1.9 X.509

- ITU-T-X.509, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute Certificate frameworks (available at: https://www.itu.int/rec/T-REC-X.509/en)
- ISO/IEC 9594-8, Information technology—Open Systems Interconnection—The Directory—Part 8: The Directory: Public-key and attribute Certificate frameworks (available at:https://www.iso.org/standard/80325.html)
- IETF-RFC-5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

2.2 Cryptographic methods

This specification targets a 128-bit security level for all cryptographic primitives. The cryptographic methods used by this specification are shown in Table 4 in *Section 3.2, Certificates* .

2.2.1 Random number generators

The generation of cryptographic keys and the cryptographic protocol exchanges rely on cryptographic quality random numbers. Random numbers are defined as numbers that are distinguishable from random by no algorithm with an algorithmic complexity of less than $O(2^{128})$.

The output of a NIST SP800-90A-compliant PRNG seeded with a 256-bit full SP800-90B entropy value is sufficient to meet this standard.

2.3 Security overview

Security of the Authentication protocol depends on the protection of private keys, and that protection is supported by security evaluation.

2.3.1 Methodology

This specification defines a Certificate-based method for Authentication that allows a Power Receiver to authenticate a Power Transmitter and, by policy, choose how to interact with that Power Transmitter. For example, a Power Receiver may choose not to use the full advertised capabilities of an unauthenticated Power Transmitter.

2.3.2 Periodic re-Authentication

The Power Receiver can optionally perform periodic re-Authentications to verify that an authenticated Power Transmitter has not been replaced by a different one.

2.4 Impact to existing ecosystem

The impact to existing Power Transmitter Products depends largely on individual Policy decisions regarding legacy Power Transmitters (i.e. Power Transmitters that predate this specification). For example, a Power Receiver with a Policy that allows full functioning of legacy Power Transmitters will have a minimal impact on the current ecosystem, while a Power Receiver with a Policy that limits or refuses to use functionalities exposed by a legacy Power Transmitter will have a more significant impact.

2.5 Support for revocation

If the Power Receiver supports Authentication functionality, then the Power Receiver should support Revocation.

Revocation Lists are normally updated off line, e.g. as part of a software or firmware update or during Product manufacturing. Manufacturers are not required to provide on-line maintenance of Revocation Lists or to make Revocation Lists field-updatable in their Products, however, the Power Receiver should frequently update its revocation list and not only during firmware updates. For some Power Receiver Products with Internet connectivity (e.g. smartphones), frequent Revocation List updates should be relatively easy. Other Power Receiver Products without direct Internet connectivity, such as fitness trackers, may not be able to update their Revocation List as frequently, but manufacturers should consider ways to keep the Revocation List current in their product designs.

Sample Document
get full document from standards.iteh.ai

NOTE: Support for updatable Revocation Lists implies field-updatable non-volatile memory.

NOTE: The WPC Authentication License Administrator (WPC-ALA) will issue Revocation Lists from time to time. The format of Revocation Lists and how they are communicated is outside the scope of this specification.