

INTERNATIONAL STANDARD

NORME INTERNATIONALE

**Qi Specification version 2.0 –
Part 9: Authentication Protocol**

**Spécification Qi version 2.0 –
Partie 9: Protocole d'authentification**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2025 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

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 It also gives information on projects, replaced and withdrawn publications.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.

Warning! Make sure that you obtained this publication from an authorized distributor.

Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.



IEC 63563-9

Edition 1.0 2025-02

INTERNATIONAL STANDARD

**Qi Specification version 2.0 –
Part 9: Authentication Protocol**

Sample Document

get full document from standards.iteh.ai

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 29.240.99; 35.240.99

ISBN 978-2-8327-0192-8

Warning! Make sure that you obtained this publication from an authorized distributor.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

QI SPECIFICATION VERSION 2.0 –

Part 9: Authentication Protocol

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 63563-9 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, Authentication Protocol* and was submitted as a Fast-Track document.

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

Draft	Report on voting
100/4253/FDIS	100/4284/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.

Sample Document

get full document from standards.iteh.ai



Qi Specification

Authentication Protocol

Sample Document

get full document from standards.iteh.ai

Version 2.0

April 2023

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.

Sample Document

get full document from standards.iteh.ai

Table of Contents

1 General	3
1.1 Structure of the Qi Specification.....	3
1.2 Scope	4
1.3 Compliance.....	4
1.4 References.....	4
1.5 Conventions	5
1.6 Power Profiles.....	7
2 Overview	8
2.1 References.....	9
2.2 Cryptographic methods	11
2.3 Security overview	11
2.4 Impact to existing ecosystem	11
2.5 Support for revocation	12
3 Certificates and private keys	13
3.1 Certificate Chains	13
3.2 Certificates.....	15
3.3 Certificate Chain slots	25
3.4 Power Transmitter private keys	26
3.5 Other private keys.....	26
4 Authentication protocol.....	27
4.1 Digest query	27
4.2 Certificate Chain read	27
4.3 Authentication challenge.....	28
4.4 Errors and alerts.....	28
5 Authentication messages	29
5.1 Authentication message header	30
5.2 Authentication requests	31
5.3 Authentication responses	34
6 Timing requirements	39
6.1 Power Receiver timing requirements.....	39
6.2 Power Transmitter timing requirements.....	40
7 Protocol flow examples	41
7.1 Simple flow	41

7.2	Flow with caching	42
7.3	Flow with caching and revocation	43
7.4	Challenge first flow.....	44

8 Cryptographic examples (informative) 46

8.1	X.509 Certificate basics	46
8.2	Dummy Root CA Certificate.....	47
8.3	Manufacturer CA Certificate Example.....	50
8.4	Example Product Unit Certificates.....	53
8.5	Certificate Chain and digest of certificates example	59
8.6	Authentication examples.....	62

Annex A: Sample data 77

A.1	Dummy Root CA Certificate in PEM format	77
A.2	Dummy Root CA Certificate in ASN.1 parser output	78
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	83
A.6	Product Unit Certificate, example 1 in ASN.1 parser output	84
A.7	Product Unit Certificate, example 2 in PEM format	86
A.8	Product Unit Certificate, example 2 in ASN.1 parser output	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. 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

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>.

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.

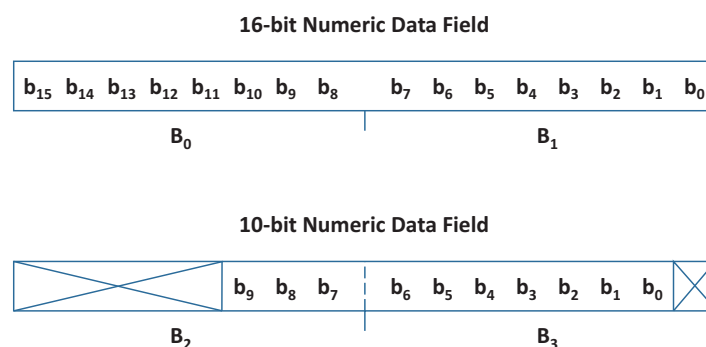
1.5.3 Fields in a data packet

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



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

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. $P_L^{(pot)} = 5 \text{ W}$.
- *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
Ax or Bx design	Yes	Yes	No	N/A	N/A
MP-Ax or MP-Bx 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

Sample Document

get full document from standards.iteh.ai

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.

Sample Document

get full document from standards.iteh.ai