IEC 63563-9

Edition 1.0 2025-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Qi Specification version 2.0 – Part 9: Authentication Protocol

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

ICS 29.240.99, 35.240.99

ISBN 978-2-8327-0545-2

IEC 63563-9:2025-02(en-fr)



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 It also gives information on projects, replaced and withdrawn publications.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

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

Authentication Protocol

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.

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

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, 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.

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SPÉCIFICATION QI VERSION 2.0 –

Partie 9: Protocole d'authentification

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'IEC n'a pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié tout ou partie de tels droits de propriété.

L'IEC 63563-9 a été établie par le Domaine Technique 15: Wireless Power Transfer, du comité d'études de l’IEC 100: Systèmes et équipements audio, vidéo et multimédia. Il s'agit d'une Norme internationale.

Il est basé sur la *Spécification Qi version 2.0, Protocole d'authentification* et a été soumis en tant que document Fast-Track.

La présente version bilingue (2025-07) correspond à la version anglaise monolingue publiée en 2025-02.

La version française de cette norme n'a pas été soumise au vote.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

La structure et les règles éditoriales utilisées dans cette publication reflètent la pratique de l'organisation qui l'a soumise.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications/.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

WIRELESS POWER

CONSORTIUM

Spécification Qi

Protocole d'authentification

Version 2.0

avril 2023

CLAUSE DE NON-RESPONSABILITÉ

Les informations contenues dans le présent document sont considérées comme exactes à la date de publication, mais elles sont fournies "en l'état" et peuvent contenir des erreurs. Le Wireless Power Consortium ne donne aucune garantie, expresse ou implicite, concernant le présent document et son contenu, y compris toute garantie de titre, de propriété, de qualité marchande ou d'adéquation à une utilisation ou un objectif particulier. Ni le Wireless Power Consortium, ni aucun membre du Wireless Power Consortium ne pourra être tenu responsable des erreurs contenues dans le présent document ou des dommages, y compris indirects ou consécutifs, résultant de l'utilisation ou de la confiance accordée à la justesse du présent document. Pour toute explication complémentaire sur le contenu du présent document, ou en cas d'incohérence ou d'ambiguïté d'interprétation perçue, contactez : info@wirelesspowerconsortium.com.

HISTORIQUE DE LA PUBLICATION

Version de la spécification	Date de sortie	Description
v2.0	avril 2023	Publication initiale de la spécification Qi v2.0.

Table des matières

1 Général 8
1.1 Structure du Qi Spécification 8
1.2 Domaine d'application 9
1.3 Conformité 9
1.4 Références 9
1.5 Conventions 10
1.6 Power Profiles 12

2 Vue d'ensemble 13
2.1 Références 14
2.2 Cryptographique méthodes 16
2.3 Aperçu de la sécurité 16
2.4 Impact sur l'écosystème existant 16
2.5 Soutien à la révocation 17

3 Certificats et clés privées 18
3.1 Chaînes de certificats 18
3.2 Certificats 20
3.3 Créneaux de la chaîne de certificats 30
3.4 Emetteur de puissance privé touches 31
3.5 Autres clés privées 31

4 Protocole d'authentification 32
4.1 Requête digest 32
4.2 Lecture de la chaîne de certificats 32
4.3 Défi d'authentification 33
4.4 Erreurs et alertes 33

5 Messages d'authentification 34
5.1 En-tête du message d'authentification 35
5.2 Demandes d'authentification 36
5.3 Réponses d'authentification 39

6 Temporisation exigences. 44
6.1 Calage du récepteur d'alimentation exigences. 44
6.2 Calage du transmetteur de puissance exigences. 45

7 Exemples de flux de protocoles 46
7.1 Flux simple 46

7.2 Flux avec cache 48
7.3 Flux avec cache et révocation 50
7.4 Défi premier flux 52

8 Exemples cryptographiques (informatif) 55
8.1 X.509 Certificate basics 55
8.2 A CA racine fictive Certificat 56
8.3 Exemple de certificat de l'autorité de certification du fabricant 59
8.4 Exemple d'unité de produit Certificats 62
8.5 Chaîne de certificats et condensé de certificats exemple 68
8.6 Exemples d'authentification 71

Annexe A : Échantillon données. 86
A.1 Certificat Root CA factice en PEM format 86
A.2 Certificat d'AC racine factice dans l'analyseur ASN.1 sortie 87
A.3 Certificat de l'autorité de certification du fabricant en PEM Format 89
A.4 Certificat de l'autorité de certification du fabricant dans l'analyseur ASN.1 output ... 90
A.5 Certificat d'unité de produit, exemple 1 en PEM format 92
A.6 Certificat d'unité de produit, exemple 1 dans l'analyseur ASN.1 sortie 93
A.7 Certificat d'unité de produit, exemple 2 en PEM format 95
A.8 Certificat d'unité de produit, exemple 2 dans l'analyseur ASN.1 output 96

1 Général

Le Wireless Power Consortium (WPC) est une organisation mondiale qui vise à développer et à promouvoir des normes mondiales pour le transfert d'énergie sans fil dans divers domaines d'application. Un premier domaine d'application comprend les appareils à surface plane tels que les téléphones mobiles et les chargeurs dans le profil de puissance de base (jusqu'à 5 W) et le profil de puissance étendu (plus de 5 W).

1.1 Structure du Qi Spécification

Documents généraux

- Introduction
- Glossaire, acronymes et symboles

Documents de description du système

- Mécanique, thermique et interface usager [domaine des transports].
- Fourniture d'énergie
- Couche physique des communications
- Protocole de communication
- Détection des objets étrangers
- Protection des étiquettes NFC
- Protocole d'authentification

1.2 Domaine d'application

La *Spécification Qi, Protocole d'authentification* (le présent document) définit l'architecture et la messagerie au niveau de l'application pour l'authentification d'un produit émetteur de puissance par un récepteur de puissance afin d'assurer que le produit émetteur de puissance est à la fois certifié Qi et le produit d'un fabricant enregistré.

1.3 Conformité

Toutes les dispositions de la *Spécification Qi* sont obligatoires, à moins qu'il ne soit spécifiquement indiqué qu'elles sont recommandées, facultatives, qu'il s'agit d'une note, d'un exemple ou d'une information. L'expression verbale des dispositions de la présente Disposition suit les règles prévues dans les Directives ISO/CEI, Partie 2.

Tableau 1 : Formes verbales pour l'expression des dispositions

Disposition	Forme verbale
Exigence	"doit" ou "ne doit pas"
Recommandation	"doit" ou "ne doit pas".
autorisation	"peut" ou "ne peut pas".
capacité	"peut" ou "ne peut pas".

1.4 Références

Pour les références non datées, le document publié le plus récent s'applique. Les publications les plus récentes du CMP peuvent être téléchargées à partir de http://www.wirelesspowerconsortium.com..