IEC 63563-9

Edition 1.0 2025-02

NORME INTERNATIONALE

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(fr)

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

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

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.

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

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..

1.5 Conventions

1.5.1 Notation des nombres

- Les nombres réels utilisent les chiffres de 0 à 9, une virgule et éventuellement une partie exponentielle.
- Les nombres entiers en notation décimale utilisent les chiffres de 0 à 9.
- Les nombres entiers en notation hexadécimale utilisent les chiffres hexadécimaux de 0 à 9 et de A à F, et sont précédés de "0x", sauf indication contraire explicite.
- Les valeurs à un seul bit utilisent les mots ZERO et ONE.

1.5.2 Tolérances

Sauf indication contraire, toutes les valeurs numériques dans la *Spécification Qi* sont exactement telles que spécifiées et ne comportent aucune tolérance implicite.

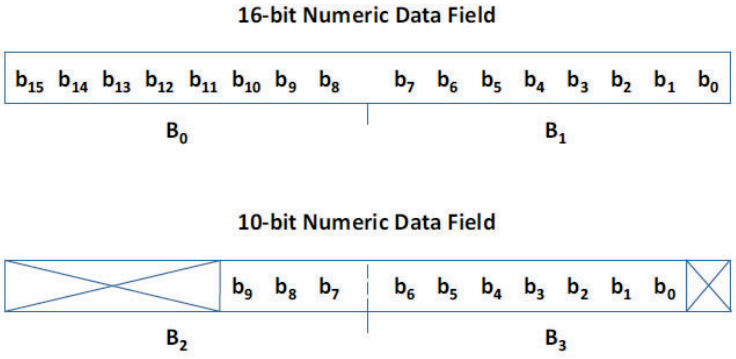
1.5.3 Champs d'un paquet de données

Une valeur numérique stockée dans un champ d'un paquet de données utilise un format big-endian. Les bits les plus significatifs sont stockés à un décalage d'octet inférieur à celui des bits les moins significatifs. Tableau 2 et Figure 1 fournissent des exemples d'interprétation de tels champs..

Tableau 2 : Exemple de champs dans un paquet de données

<table>
<tr><th></th><th>b_7</th><th>b_6</th><th>b_5</th><th>b_4</th><th>b_3</th><th>b_2</th><th>b_1</th><th>b_0</th></tr>
<tr><td>B_0</td><td colspan="8" rowspan="2">(msb)
Champ de données numériques de 16 bits
(lsb)</td></tr>
<tr><td>B_1</td></tr>
<tr><td>B_2</td><td colspan="5">Autre domaine</td><td colspan="3">(msb)</td></tr>
<tr><td>B_3</td><td colspan="6">Champ de données numériques de 10 bits</td><td>(lsb)</td><td>Champ d'application</td></tr>
</table>

Figure 1. Exemples de champs dans un paquet de données



Anglais	Français
16-bit Numeric Data field	Champ de données numériques de 16 bits
10-bit Numeric Data field	Champ de données numériques de 10 bits

1.5.4 Notation des chaînes de texte

Les chaînes de texte consistent en une séquence de caractères ASCII imprimables (c'est-à-dire compris entre 0x20 et 0x7E) entre guillemets ("). Les chaînes de texte sont stockées dans les champs des structures de données, le premier caractère de la chaîne se trouvant à l'octet de décalage le plus bas, et sont complétées par des caractères ASCII NUL (0x00) jusqu'à la fin du champ, si nécessaire.

EXEMPLE : La chaîne de texte "WPC" est stockée dans une zone de six octets sous la forme d'une séquence de caractères "W", "P", "C", NUL, NUL et NUL. La chaîne de texte "M:4D3A" est enregistrée dans un champ de six octets sous la forme de la séquence "M", " :", "4", "D", "3" et "A".

1.5.5 Notation abrégée pour les paquets de données

Dans de nombreux cas, la *Spécification Qi* fait référence à un paquet de données en utilisant la notation abrégée suivante :

<MNEMONIC>/<modificateur>

Dans cette notation,<MNEMONIQUE>fait référence au mnémonique du paquet de données défini dans la *Spécification Qi, Protocole de communication*, et<modificateur>fait référence à une valeur particulière dans un champ du paquet de données. Les définitions des paquets de données dans la *Spécification Qi, Protocole de communication*, énumèrent les significations des modificateurs.

Par exemple, EPT/cc désigne un paquet de données de fin de transfert de puissance dont le champ de code de fin de transfert de puissance est réglé sur 0x01.

1.6 Power Profiles

Un profil de puissance détermine le niveau de compatibilité entre un émetteur de puissance et un récepteur de puissance. Tableau 3 définit les profils de puissance disponibles.

- *BPP PTx*: Un émetteur de puissance à profil de puissance de base.
- *EPP5 PTx*: Un émetteur de puissance à profil de puissance étendu ayant une capacité de transfert de puissance restreinte, c'est-à-dire $P_L^{(pot)}$ = 5 W..
- *EPP PTx*: Un émetteur de puissance à profil de puissance étendu.
- *BPP PRx*: Un profil de puissance de base Récepteur de puissance.
- *EPP PRx*: Un récepteur de puissance à profil de puissance étendu.

Tableau 3 : Capacités incluses dans un profil de puissance

Le phénomène	BPP PTx	EPP5 PTx	EPP PTx	BPP PRx	EPP PRx
A*x* ou B*x* design	Oui	Oui	Non	N/A	N/A
MP-A*x* ou MP-B*x* design	Non	Non	Oui	N/A	N/A
Protocole de base	Oui	Oui	Oui	Oui	Oui
Protocole étendu	Non	Oui	Oui	Non	Oui
Authentification	N/A	En option	Oui	N/A	En option

2 Vue d'ensemble

La *Spécification Qi, Protocole d'authentification* (le présent document) définit un protocole permettant à un récepteur de puissance d'authentifier un émetteur de puissance. Dans ce contexte, l'authentification est une méthode inviolable pour établir et vérifier l'identité de l'émetteur de puissance, permettant au récepteur de puissance de faire confiance à l'émetteur de puissance pour fonctionner dans les limites de la *spécification Qi*. Ce protocole d'authentification version 1.0 utilise les flux de transport de données entre le récepteur de puissance et l'émetteur de puissance tels que définis dans la *Spécification Qi, Protocole de communication*.

L'authentification permet à une organisation de définir et d'appliquer une politique concernant les produits acceptables. Cela permettra d'obtenir des garanties de sécurité utiles dans des situations réelles. Par exemple, un fabricant de téléphones mobiles préoccupé par les dommages au produit ou les limites de sécurité résultant de dispositifs de chargement sans fil non conformes aux normes peut établir une politique limitant la puissance tirée d'un chargeur sans fil non fiable.

Le présent document vise à s'aligner étroitement sur la spécification relative à l'authentification USB, d'autant plus qu'il est probable qu'il existe sur le marché des produits prenant en charge les deux types de spécification.

Outre ce document, le *WPC Manufacturer Agreement* couvre les exigences juridiques et de mise en œuvre, notamment le stockage et le traitement sécurisés des secrets (Annexe A) ainsi que les règles et la procédure de révocation (Annexe B). Pour de plus amples informations ou pour obtenir une copie de cet accord, veuillez contacter : info@wirelesspowerconsortium.com.

2.1 Références

Sauf indication contraire, toutes les normes spécifiées, y compris celles de l'ISO, de l'UIT et du NIST, font référence à la version ou à l'édition la plus récente, au 1er janvier 2018.

ECDSA

- ANSI X9.62-2005 ; Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA) (disponible sur www.global.ihs.com or https:// www.techstreet.com)
- NIST-FIPS-186-4, Norme de signature numérique (DSS), Section 6, Publication des normes fédérales de traitement de l'information, juillet 2013 (disponible à l'adresse suivante : http://nvlpubs.nist.gov/nistpubs/FIPS/ NIST.FIPS.186-4.pdf)
- ISO/IEC 14888-3 Signatures numériques avec annexe - Partie 3 : Mécanismes basés sur le logarithme discret (Article 6.6)

NIST P-256, secp-256r1

- NIST-FIPS-186-4, Norme de signature numérique (DSS), Annexe D : Courbes elliptiques recommandées pour l'utilisation par le gouvernement fédéral, Publication des normes fédérales de traitement de l'information, juillet 2013 (disponible à l'adresse suivante : http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).
- ISO/IEC 15946 Techniques cryptographiques basées sur les courbes elliptiques (NIST P-256 est inclus comme exemple)

NOTE : La série ISO/IEC 15946 traite les courbes elliptiques différemment de la norme FIPS 186-4. L'IEC 15946-5 porte sur la génération de courbes elliptiques. En d'autres termes, sur la base de la méthode décrite dans la Partie 5, chaque application et mise en œuvre peut générer ses propres courbes à utiliser. En d'autres termes, il n'existe pas de courbes recommandées par l'ISO/CEI. P-256 est pris en considération dans la norme ISO/IEC 15946. En outre, les signatures par courbes elliptiques et les systèmes d'établissement de clés ont été transférés respectivement dans les normes ISO/IEC 14888 et ISO/IEC 11770, ainsi que d'autres mécanismes basés sur le logarithme discret. Des vecteurs de test (exemples) utilisant le P-256 sont inclus pour chacun de ces mécanismes.

SEC 1

- Certicom Corp, Groupe des normes de cryptographie efficace (SECG), SEC 1 : "Elliptic Curve Cryptography," Version 1.0, Septembre 2000 (disponible à l'adresse : https://www.secg.org/SEC1-Ver- 1.0.pdf)

SEC 2

- Certicom Corp, Groupe des normes de cryptographie efficace (SECG), SEC 2 : "Paramètres recommandés pour le domaine des courbes elliptiques", version 2.0, janvier 2010 (disponible à l'adresse suivante : http:// www.secg.org/sec2-v2.pdf)