



**BSI Standards Publication**

## **Qi Specification version 2.0**

---

Part 9: Authentication Protocol

## National foreword

This British Standard is the UK implementation of EN IEC 63563-9:2025. It is identical to IEC 63563-9:2025.

The UK participation in its preparation was entrusted to Technical Committee EPL/100, Audio-visual equipment.

A list of organizations represented on this committee can be obtained on request to its committee manager.

### Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025  
Published by BSI Standards Limited 2025

ISBN 978 0 539 31165 5

ICS 29.240.99; 35.240.99

**Compliance with a British Standard cannot confer immunity from legal obligations.**

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2025.

### Amendments/corrigenda issued since publication

| Date | Text affected |
|------|---------------|
|------|---------------|

English Version

Qi Specification version 2.0 - Part 9: Authentication Protocol  
(IEC 63563-9:2025)

Spécification Qi version 2.0 - Partie 9: Protocole  
d'authentification  
(IEC 63563-9:2025)

Qi Spezifikation Version 2.0 - Teil 9: Authentifizierung  
Protokoll  
(IEC 63563-9:2025)

This European Standard was approved by CENELEC on 2025-03-21. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

## **European foreword**

The text of document 100/4253/FDIS, future edition 1 of IEC 63563-9, prepared by TC 100/Technical Area 15 "Wireless Power Transfer" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 63563-9:2025.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2026-03-31 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2028-03-31 document have to be withdrawn

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

## **Endorsement notice**

The text of the International Standard IEC 63563-9:2025 was approved by CENELEC as a European Standard without any modification.

## 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](http://www.iec.ch/members_experts/refdocs). The main document types developed by IEC are described in greater detail at [www.iec.ch/publications](http://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](http://webstore.iec.ch) in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.



## **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](mailto: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

|                                                |           |
|------------------------------------------------|-----------|
| <b>1 General .....</b>                         | <b>3</b>  |
| 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         |
| <b>2 Overview .....</b>                        | <b>8</b>  |
| 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        |
| <b>3 Certificates and private keys .....</b>   | <b>13</b> |
| 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        |
| <b>4 Authentication protocol.....</b>          | <b>27</b> |
| 4.1 Digest query .....                         | 27        |
| 4.2 Certificate Chain read .....               | 27        |
| 4.3 Authentication challenge.....              | 28        |
| 4.4 Errors and alerts.....                     | 28        |
| <b>5 Authentication messages .....</b>         | <b>29</b> |
| 5.1 Authentication message header .....        | 30        |
| 5.2 Authentication requests .....              | 31        |
| 5.3 Authentication responses .....             | 34        |
| <b>6 Timing requirements .....</b>             | <b>39</b> |
| 6.1 Power Receiver timing requirements.....    | 39        |
| 6.2 Power Transmitter timing requirements..... | 40        |
| <b>7 Protocol flow examples .....</b>          | <b>41</b> |
| 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>.

# 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.

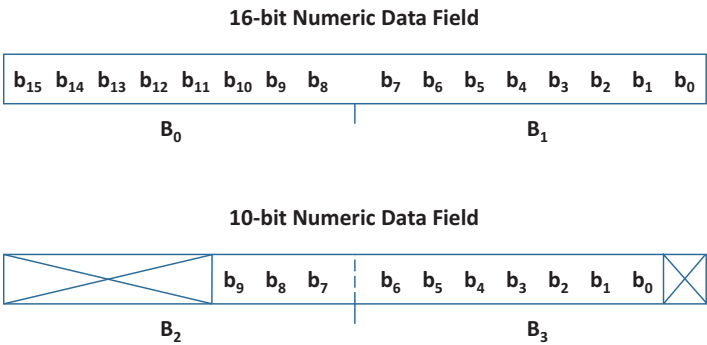
## 1.5.3 Fields in a data packet

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 <sub>7</sub>                        | b <sub>6</sub> | b <sub>5</sub> | b <sub>4</sub> | b <sub>3</sub> | b <sub>2</sub> | b <sub>1</sub> | b <sub>0</sub> |
|----------------|---------------------------------------|----------------|----------------|----------------|----------------|----------------|----------------|----------------|
| B <sub>0</sub> | (msb) 16-bit Numeric Data Field (lsb) |                |                |                |                |                |                |                |
| B <sub>1</sub> |                                       |                |                |                |                |                |                |                |
| B <sub>2</sub> | Other Field                           |                |                |                |                | (msb)          |                |                |
| B <sub>3</sub> | 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 field 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.  $P_L^{(pot)} = 5 \text{ W}$ .
- *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 |

## 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](mailto: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](http://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>)

**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)

**SP800-90A**

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

**SP800-90B**

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

**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)

**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 5 \(in Section 3.1\)](#).

### 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.

**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.

## 3 Certificates and private keys

### 3.1 Certificate Chains

The requirements in this section apply to Certificate Chains that are populated in slots 0 and 1. The Power Transmitter Product manufacturer determines the requirements for Certificates that are populated in slots 2 and 3. For further information about slots, see [Section 3.3, Certificate Chain slots](#).

A Certificate Chain consists of three Certificates; see [Table 4](#). The first Certificate in the chain is the Root Certificate identifying the WPC Root Certificate Authority. It is a self-signed Certificate (i.e. signed by the WPC Root Certificate Authority). As an optimization, the Certificate Chain contains a hash of the Root Certificate rather than the Root Certificate itself. The second Certificate is a Manufacturer CA Certificate identifying the product's manufacturer. It is signed by the WPC Root Certificate Authority. The last Certificate in the chain is a Product Unit Certificate identifying the individual Power Transmitter product. It is signed by the Manufacturer Certificate Authority.

In addition to identification data, the Manufacturer CA Certificate contains a public key for verifying the authenticity of the Product Unit Certificate. The Product Unit Certificate contains a public key for verifying the authenticity of the Power Transmitter Product Unit. See [Section 4, Authentication protocol](#), for details.

The following requirements apply to the Certificates in a Certificate Chain.

- Each Product Unit Certificate shall identify a unique Power Transmitter Product Unit by using, for example, the product unit's RSID number (wpc-qi-rsid).
- Each Power Transmitter Product Unit shall have a unique public key.
- Product Unit Certificates contained in different slots of the same Power Transmitter Product Unit may contain the same identity and public key, provided that this does not introduce a security vulnerability.
- A manufacturer may have multiple Manufacturer CA Certificates to identify, for example, different production facilities or product families. Each of these Manufacturer CA Certificates shall contain a unique public key relating to a unique private key.

**NOTE:** Using multiple Manufacturer CA Certificates is encouraged to partition volumes of product units to limit the collateral impact caused in the event that a Manufacturer CA Certificate is revoked (collateral impact of revoking all product units signed by that Manufacturer CA Certificate).

- A manufacturer shall use the private key associated with a Manufacturer CA Certificate to sign Product Unit Certificates.
- The WPC Root Certificate Authority shall ensure that all Manufacturer CA Certificates contain unique public keys.

The Certificate Chains populated in slots 0 and 1 shall use X.509 Certificates. See [Section 3.3, Certificate Chain slots](#), for further information about slots 0 and 1.

**Table 4: Certificate Chain (X.509 Certificates)**

|                                                                                                         | $b_7$                                         | $b_6$  | $b_5$ | $b_4$ | $b_3$ | $b_2$ | $b_1$ | $b_0$ |
|---------------------------------------------------------------------------------------------------------|-----------------------------------------------|--------|-------|-------|-------|-------|-------|-------|
| $B_0 \dots B_1$                                                                                         | msb                                           | Length |       |       |       |       |       |       |
|                                                                                                         |                                               |        |       |       |       |       |       | lsb   |
| $B_2 \dots B_{(1+N\_RH)}$                                                                               | Root Certificate Hash (length $N\_RH$ )       |        |       |       |       |       |       |       |
| $B_{(2+N\_RH)} \dots B_{(1+N\_RH+N\_MC)}$                                                               | Manufacturer CA Certificate (length $N\_MC$ ) |        |       |       |       |       |       |       |
| $B_{(2+N\_RH+N\_MC)} \dots B_{(1+N\_RH+N\_MC+N\_PUC)}$                                                  | Product Unit Certificate (length $N\_PUC$ )   |        |       |       |       |       |       |       |
| <b>Note:</b> The Root Certificate is not included in the chain, only its hash is included in the chain. |                                               |        |       |       |       |       |       |       |

**Length** The length is the total number of bytes in the Certificate Chain including the Length field.

**Root Certificate Hash** A SHA-256 hash of the Root Certificate. The length of  $N\_RH$  is 32 bytes. See [Section 2, Overview](#).

**Manufacturer CA Certificate** This Certificate identifies the manufacturer.

**Product Unit Certificate** This Certificate identifies the individual product unit.

## 3.2 Certificates

### 3.2.1 Format of Certificates

All Certificates shall use:

- the X.509 v3 ASN.1 structure,
- binary DER encoding for ASN.1, and
- the cryptographic methods listed in [Table 5](#).

**Table 5: Summary of cryptographic methods**

| Method                                                                                                                                                    | Use                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| X.509 v3, DER encoding                                                                                                                                    | Certificate format                                                                                            |
| ECDSA using the NIST P256, secp256r1 curve, uncompressed point OR compressed point format as specified by SEC1 (see <a href="#">Section 2, Overview</a> ) | Digital signing of Certificates and Authentication Messages                                                   |
| SHA-256                                                                                                                                                   | Hash algorithm, used in the ECDSA calculation and in creating digests of Certificates and Certificate Chains. |

The further description of the Certificate format assumes that the reader is familiar with X.509 v3 Certificate terminology.

**NOTE:** Certificates and the fields, attributes, and extensions defined therein are Big Endian.

Product unit Certificates shall not exceed MaxProdCertSize in length. A Manufacturer CA Certificate shall not exceed MaxManufacturerCertSize in length.

#### 3.2.1.1 Textual format

All textual ASN.1 objects contained within X.509 Certificates, including DirectoryString, GeneralName, and DisplayText, shall be specified as a UTF8String. The length of any textual object shall not exceed 64 bytes excluding the DER type and DER length encoding.

#### 3.2.1.2 Attributes and Extensions

Where applicable, the Object Identifier (OID) is provided.

##### Basic Constraints (OID 2.5.29.19)

Manufacturer CA Certificates contain this extension. (The extension is marked as critical, its cA component is set to true, and its pathLenConstraint component set to zero). Product Unit Certificates do not contain this extension.

### Validity

The notBefore and notAfter fields indicate the time interval during which information regarding a Certificate's validity is maintained. For Product Units, the validity times should be ignored.

Certificate notBefore and notAfter validity times shall be specified using ASN.1 GeneralizedTime for any year, or ASN.1 UTCTime for years prior to 2050.

For a Manufacturer CA Certificate it is recommended that the notBefore field be "19700101000000Z" (for 00:00 on 01-Jan-1970 UTC, which is POSIX epoch time). It is recommended that the notAfter field be "99991231235959Z" (for 23:59:59 on 31-Dec-9999 UTC, which is used for an unknown expiration time as defined in IETF-RFC-5280, Section 4.1.2.5). Use of the recommended notBefore and notAfter values will maximize compatibility with Certificate processing stacks.

### Qi policy extension (wpc-qi-policy)

The WPC Qi policy extension is a custom Manufacturer CA Certificate extension for use with products compliant to this specification. The value is a binary object and is reserved in this version of the specification. The value of wpc-qi-policy is listed on [The Qi Specifications](#) page of the WPC members' website.

The binary object is encoded as an ASN.1 DER OCTET STRING with a fixed size of QiPolicySize bytes.

Manufacturer CA Certificates shall contain this extension. Product Unit Certificates shall not contain this extension.

### Qi RSID extension (wpc-qi-rsid)

The WPC Qi revocation sequential identifier (RSID) extension is a custom Product Unit Certificate extension for use with products compliant to this specification. The value is a binary object and is provided to store a sequential identifier unique to each product unit that enables range-based revocation of batches. The value of wpc-qi-rsid is listed on [The Qi Specifications](#) page of the WPC members' website.

The binary object is DER encoded as an ASN.1 OCTET STRING with a maximum size of MaxQiRSIDSize bytes. The RSID value is unique to each product unit, from a minimum of 1 up to MaxQiRSIDSize bytes.

Product Unit Certificates shall contain this extension. Manufacturer CA Certificates shall not contain this extension.

### ASN.1 schema for WPC Object identifiers

The ASN.1 module below defines the WPC administered object identifiers and the schema for the certificate extensions used for WPC Qi authentication.

```
-- WPC OID allocation

wpc INTEGER ::= 148

id-wpc OBJECT IDENTIFIER

    ::= {joint-iso-ccitt(2) international-organizations(23) wpc}

-- Qi Authentication certificate extensions

qiAuth INTEGER ::= 1

id-wpc-qiAuth OBJECT IDENTIFIER ::= {id-wpc qiAuth}

policy INTEGER ::= 1

id-wpc-qiAuth-policy OBJECT IDENTIFIER ::= {id-wpc-qiAuth policy}

rsid INTEGER ::= 2

id-wpc-qiAuth-rsid OBJECT IDENTIFIER ::= {id-wpc-qiAuth rsid}

-- WPC Qi Authentication size constants

wpcQiAuthPolicySize INTEGER ::= 4

wpcQiAuthRsidMaxSize INTEGER ::= 9

-- WPC Qi Authentication certificate extension schema

policy ::= OCTET STRING (SIZE (wpcQiAuthPolicySize))

rsid ::= OCTET STRING (SIZE (1..wpcQiAuthRsidMaxSize))
```

#### 3.2.1.3 Manufacturer CA Certificate

A Manufacturer CA Certificate uses the ASN.1 structure defined in Rec. ITU-T X.509 (10/2016), Section 7.2 Public-Key Certificate.

The TBSCertificate component of a Manufacturer CA Certificate only implements the ASN.1 fields shown in [Table 6](#).

**Table 6: Certificate profile for a Manufacturer CA Certificate**

|                | Field              | OID                                                                                                                                                                                                                                                         | Data type                                                                | Value                                                                                                                                                                                                                                | Example                      |
|----------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| TBSCertificate | Version            |                                                                                                                                                                                                                                                             | INTEGER                                                                  | 0x02 {=X.509v3}                                                                                                                                                                                                                      | 0x02                         |
|                | SerialNumber       |                                                                                                                                                                                                                                                             | INTEGER                                                                  | A unique 1- to 72-bit positive integer value                                                                                                                                                                                         | 0x01 10 20 30 40 50<br>60 70 |
|                |                    | <b>Note:</b> The maximum length of 9 bytes refers to the “baseband” original value, before DER encoding. The encoded value can have an additional zero byte if the top bit of the original value is set. Be aware that this can be 10 bytes after encoding. |                                                                          |                                                                                                                                                                                                                                      |                              |
|                | signature          | 1.2.840.10045.4.3.2<br>{ecdsa-with-SHA256}                                                                                                                                                                                                                  |                                                                          | N/A                                                                                                                                                                                                                                  |                              |
|                | issuer             | 2.5.4.3<br>{Common Name}                                                                                                                                                                                                                                    | UTF8String                                                               | “WPCCA”+ one character suffix denoting different root CA instances                                                                                                                                                                   | “WPCCA1”                     |
|                | validity.notBefore |                                                                                                                                                                                                                                                             | Either Generalized Time for any year, or UTCTime for years prior to 2050 | Any value (not used by PRx)                                                                                                                                                                                                          | 2000-01-01 00:00:00          |
|                | validity.notAfter  |                                                                                                                                                                                                                                                             | Either Generalized Time for any year, or UTCTime for years prior to 2050 | Any value (not used by PRx)                                                                                                                                                                                                          | 9999-12-31 23:59:59          |
|                | subject            | 2.5.4.3<br>{Common Name}                                                                                                                                                                                                                                    | UTF8String                                                               | 7 byte string consisting of: <ul style="list-style-type: none"> <li>▪ four upper-case characters containing a PTMC hex value</li> <li>▪ one character containing a dash</li> <li>▪ two arbitrary alpha-numeric characters</li> </ul> | “CACA-1A”                    |

**Table 6: Certificate profile for a Manufacturer CA Certificate (Continued)**

|               | Field                                            | OID                                 | Data type       | Value                                                                                        | Example                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------|-------------------------------------|-----------------|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TBSertificate | subjectPublicKey<br>Info.algorithm               | 1.2.840.10045.2.1<br>{ecPublicKey}  |                 | N/A                                                                                          |                                                                                                                                                                                                                                          |
|               |                                                  | 1.2.840.10045.3.1.7*<br>{secp256r1} |                 | N/A                                                                                          |                                                                                                                                                                                                                                          |
|               | subjectPublicKey<br>Info.subjectPubli<br>cKey    |                                     | BIT STRING      | (Public Key value;<br>optionally may use<br>compressed point<br>representation) <sup>†</sup> | 0x04:64:68:34:24:4e<br>:1a:37:b2:f8:3a:d5:3<br>0:68:73:8a:65:9b:e2:<br>a6:d2:c6:f3:c9:3f:90:<br>5e:8c:7d:a3:59:79:2<br>7:6b:a7:fb:d4:30:83:<br>42:a9:90:a7:c1:92:90<br>:98:20:7d:90:77:f2:9<br>7:f3:f5:3a:77:25:01:3<br>c:55:44:19:e8:4a |
|               | Extensions.1                                     | 2.5.29.19<br>{basicConstraints}     |                 | N/A                                                                                          |                                                                                                                                                                                                                                          |
|               | Extensions.1.<br>critical                        |                                     | BOOLEAN         | TRUE                                                                                         | TRUE                                                                                                                                                                                                                                     |
|               | Extensions.1.<br>extnValue.ca                    |                                     | BOOLEAN         | TRUE                                                                                         | TRUE                                                                                                                                                                                                                                     |
|               | Extensions.1.<br>extnValue.pathL<br>enConstraint |                                     | INTEGER         | 0                                                                                            | 0x00                                                                                                                                                                                                                                     |
|               | Extensions.2                                     | 2.23.148.1.1<br>{wpc-qiAuth-policy} |                 | N/A                                                                                          |                                                                                                                                                                                                                                          |
|               | Extensions.2.<br>critical                        |                                     | BOOLEAN         | TRUE                                                                                         | TRUE                                                                                                                                                                                                                                     |
|               | Extensions.2.<br>extnValue                       |                                     | OCTET<br>STRING | 4 octets (bytes) re-<br>served for future use                                                | 0x00 00 00 01                                                                                                                                                                                                                            |

\* 1.2.840.10045 refers to the named curve defined equivalently by three organizations as:  
NIST (FIPS186-4): "P-256", SECG (SEC 2): "secp256r1", and IETF (RFC 3279): "prime256v1"

<sup>†</sup> A Certificate verifier can unambiguously distinguish compressed from uncompressed point representations by evaluating the value of the first byte (0x02 and 0x03 for compressed points and 0x04 for an uncompressed point).

### 3.2.1.4 Product Unit Certificate

A Product Unit Certificate uses the ASN.1 structure defined in Rec. ITU-T X.509 (10/2016), Section 7.2 Public-Key Certificate.

The TBSCertificate component of a Product Unit Certificate only implements the ASN.1 fields shown in [Table 7](#).

**Table 7: Certificate profile for a Product Unit Certificate**

|                | Field              | OID                                                                                                                                                                                                                                                         | Data Type                                                                | Value                                                                                                                                                                                                                                                                                                                                          | Example                      |
|----------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| TBSCertificate | Version            |                                                                                                                                                                                                                                                             | INTEGER                                                                  | 0x02<br>{=X.509v3}                                                                                                                                                                                                                                                                                                                             | 0x02                         |
|                | serialNumber       |                                                                                                                                                                                                                                                             | INTEGER                                                                  | A unique 1- to 72-bit positive integer value                                                                                                                                                                                                                                                                                                   | 0x01 10 20 30 40 50 60<br>70 |
|                |                    | <b>Note:</b> The maximum length of 9 bytes refers to the “baseband” original value, before DER encoding. The encoded value can have an additional zero byte if the top bit of the original value is set. Be aware that this can be 10 bytes after encoding. |                                                                          |                                                                                                                                                                                                                                                                                                                                                |                              |
|                | signature          | 1.2.840.10045.4.3.2<br>{ecdsa-with-SHA256}                                                                                                                                                                                                                  |                                                                          | N/A                                                                                                                                                                                                                                                                                                                                            |                              |
|                | issuer             | 2.5.4.3<br>{Common Name}                                                                                                                                                                                                                                    | UTF8String                                                               | 7 bytes string consisting of: <ul style="list-style-type: none"> <li>Four upper-case characters containing a PTMC hex value</li> <li>one character containing a dash</li> <li>two arbitrary alpha-numeric characters</li> <li>this matches exactly byte-for-byte the value from the Manufacturer CA Certificate Subject common name</li> </ul> | "CACA-1A"                    |
|                | validity.notBefore |                                                                                                                                                                                                                                                             | Either Generalized Time for any year, or UTCTime for years prior to 2050 | Should use the current time when issuing the Certificate (not used by PRx)                                                                                                                                                                                                                                                                     | 2020-10-01 00:00:00          |

**Table 7: Certificate profile for a Product Unit Certificate (Continued)**

|                | Field                          | OID                                       | Data Type                                                                | Value                                                                                                                                                                                                                                                                                                                                                                                                        | Example             |
|----------------|--------------------------------|-------------------------------------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| TBSCertificate | validity.notAfter              |                                           | Either Generalized Time for any year, or UTCTime for years prior to 2050 | Should use one day after NotBefore (not used by PRx)                                                                                                                                                                                                                                                                                                                                                         | 2020-10-02 00:00:00 |
|                | subject.attribute1             | 2.5.4.3<br>{Common Name}                  | UTF8String                                                               | String consisting of: <ul style="list-style-type: none"> <li>The Qi ID encoded as a six-character text string, left-padded with UTF-8 "0" (zero) characters as necessary. For example, the Subject ID for a product with Qi ID 6386 is encoded as "006386"</li> <li>Optionally one character containing a dash followed by up to 28 arbitrary characters to improve readability e.g. product name</li> </ul> | "006386-Model5"     |
|                | subject.attribute2 {optional}  | 2.5.4.92<br>{tagAFI}                      | OCTET STRING                                                             | Optional: up to 32 arbitrary bytes                                                                                                                                                                                                                                                                                                                                                                           | 0x20 20 09 23 F4    |
|                | subject.attribute3 {optional}  | 0.9.2342.1920<br>0300.100.1.1<br>{userId} | UTF8String                                                               | Optional: up to 32 arbitrary characters                                                                                                                                                                                                                                                                                                                                                                      | "SEPT-23"           |
|                | subjectPublicKeyInfo.algorithm | 1.2.840.10045.2.1<br>{ecPublicKey}        |                                                                          | N/A                                                                                                                                                                                                                                                                                                                                                                                                          |                     |
|                |                                | 1.2.840.10045.3.1.7*<br>{secp256r1}       |                                                                          | N/A                                                                                                                                                                                                                                                                                                                                                                                                          |                     |

**Table 7: Certificate profile for a Product Unit Certificate (Continued)**

|                | Field                                         | OID                                   | Data Type       | Value                                                                                        | Example                                                                                                                                                                                                                              |
|----------------|-----------------------------------------------|---------------------------------------|-----------------|----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TBSCertificate | subjectPublic<br>KeyInfo.subject<br>PublicKey |                                       | BIT STRING      | (Public Key value;<br>optionally may use<br>compressed point<br>representation) <sup>†</sup> | 0x04:64:68:34:24:4e:1a:<br>37:b2:f8:3a:d5:30:68:73<br>:8a:65:9b:e2:a6:d2:c6:f<br>3:c9:3f:90:5e:8c:7d:a3:5<br>9:79:27:6b:a7:fb:d4:30:<br>83:42:a9:90:a7:c1:92:90<br>:98:20:7d:90:77:f2:97:f3<br>:f5:3a:77:25:01:3c:55:4<br>4:19:e8:4a |
|                | Extensions.1                                  | 2.23.148.1.2<br>{wpc-qiAuth-<br>rsid} |                 | N/A                                                                                          |                                                                                                                                                                                                                                      |
|                | Extensions.1.<br>critical                     |                                       | BOOLEAN         | TRUE                                                                                         | TRUE                                                                                                                                                                                                                                 |
|                | Extensions.1.<br>extnValue                    |                                       | OCTET<br>STRING | RSID                                                                                         | 0x00 00 00 00 00<br>00 00 00 01                                                                                                                                                                                                      |

\* 1.2.840.10045 refers to the named curve defined equivalently by three organizations as:

NIST (FIPS186-4): "P-256"

SECG (SEC 2): "secp256r1"

IETF (RFC 3279): "prime256v1"

<sup>†</sup> A Certificate verifier can unambiguously distinguish compressed from uncompressed point representations by evaluating the value of the first byte (0x02 and 0x03 for compressed points and 0x04 for an uncompressed point).