Provisioning OPTIGA™ Trust Charge for WLC transmitters

Application note

About this document

Scope and purpose

This document is intended to provide process information for provisioning OPTIGA™ Trust Charge for wireless charger (WLC) transmitter system authentication functionality.

Intended audience

Product manufacturers who want to adopt the WLC transmitter reference design for their end product.

Table of contents

1 Introduction

This document describes the blocks in the WLC system architecture required for the Qi authentication process using OPTIGA™ Trust Charge. The Qi 1.3.x specification mandates authentication for Extended Power Profile (EPP) Power Delivery (PD) of more than 5 W.

Qi authentication is a tamper-resistant method to establish and verify the identity of the power transmitter; it enables the power receiver to trust the power transmitter to operate within the bounds of the Qi specification. OPTIGA™ Trust Charge enables the WLC power transmitter's authentication functionality and thereby ensures that the WLC transmitter system remains compliant with the Qi specification.

OPTIGA™ Trust Charge's main features are:

- Common Criteria EAL 6+ certified secure storage subsystem
- Supports X.509 v3 with DER encoding for the certificate format
- Authentication based on ECDSA
- Cryptography support: NIST P-256, SHA2
- OPTIGA™ Trust Charge meets the security and authentication requirements mandated by the WPC specification
- OPTIGA™ Trust Charge comes with manufacturer certificate service provider (MCSP) services for creating and provisioning the WPC-signed certificate chain issued to the product manufacturer organization
  - This process creates a new OPTIGA™ Trust Charge sales part number for the customer organization

2 WLC transmitters designed with OPTIGA™ Trust Charge

OPTIGA™ Trust Charge is interfaced with the WLC transmitter system processor through the I²C bus, as shown in **Figure 1**. The WLC transmitter system processor has all the hardware/firmware capabilities to use the OPTIGA™ Trust Charge for Qi authentication functionality without any additional requirements.

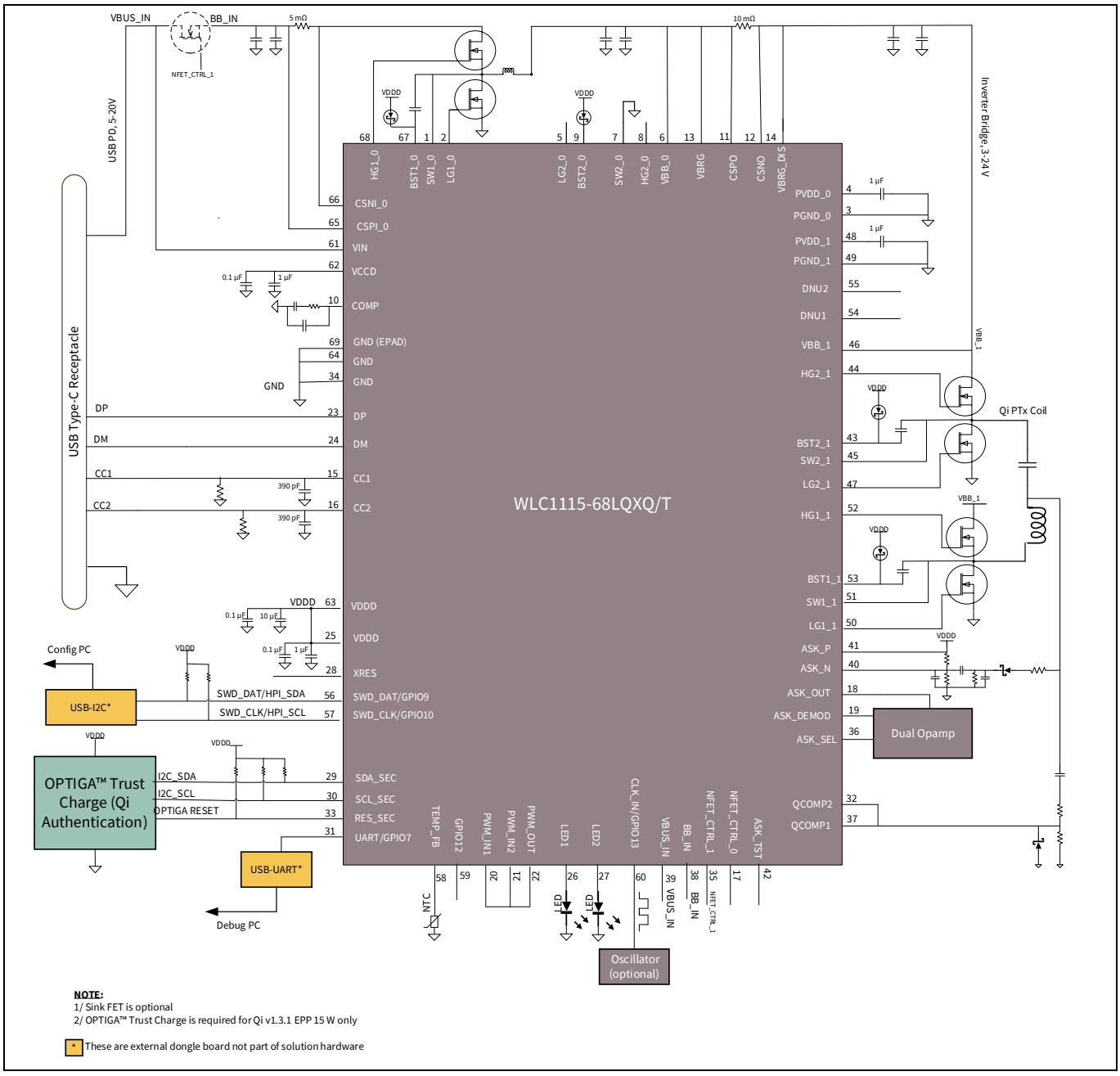

Figure 1 WLC transmitter system design

3 Public key infrastructure

The Qi specification follows the public key infrastructure (PKI), and uses the following cryptographic methods in Qi wireless charger cryptography.

Table 1 Qi wireless charger cryptography methods

Method	Use
X.509 v3, ANS.1 DER encoding	Certificate format
ECDSA using the NIST P256, secp256r1 curve	Digital signing of certificates and authentication messages
SHA-256	The hash algorithm is used in the ECDSA calculation and in creating digests of certificates and certificate chains

WPC public key cryptography (PKC) relies on a public and private key pair to encrypt and decrypt the content. These keys are mathematically related, and the content encrypted by one of the keys can be decrypted by using the other key. The private key is the most sensitive secure credential and must be stored securely. The public key is typically a part of the binary certificate, and this certificate is transmitted to the recipient through a communication medium.

The recipient of the public key certificate can do the following:

- Cryptographically verify the authenticity of public key certificate data origin
- Cryptographically verify the challenge which was signed by the “Secure Storage Subsystem” in the power transmitter

The X.509 PKI standard identifies the requirements for robust public key certificates. A public key certificate is a digitally signed data structure that binds a public key with the power transmitter device identity. Public key certificates are issued by a certificate authority (CA).

A PKI is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates. WPC defines the PKI process and rules for digitally signed certificate chain creation. See the authentication protocol booklet in the Qi specification and the WPC-PKI web page for more information.

The Qi specification mandates the power transmitter to securely host the product unit’s private key for digital signature purposes in a secure storage subsystem. This private key is used to digitally sign the Challenge Authentication response from the power transmitter device.

4 Provisioning OPTIGA™ Trust Charge

The WLC transmitter solution is a reference design for the product manufacturer adaptation. The public key certificate data present in the OPTIGA™ Trust Charge of the WLC transmitter reference design contains:

- Infineon Technologies as a power transmitter manufacturer organization
- WLC solution reference design's Qi logo certificate registration Qi-ID

Therefore, the manufacturer certificate data and product unit certificate data must be provisioned in OPTIGA™ Trust Charge to represent the product manufacturer's end products. The following flow diagram depicts the process flow involved in provisioning OPTIGA™ Trust Charge for the end-product manufacturer organization and end-product logo registration Qi-ID.

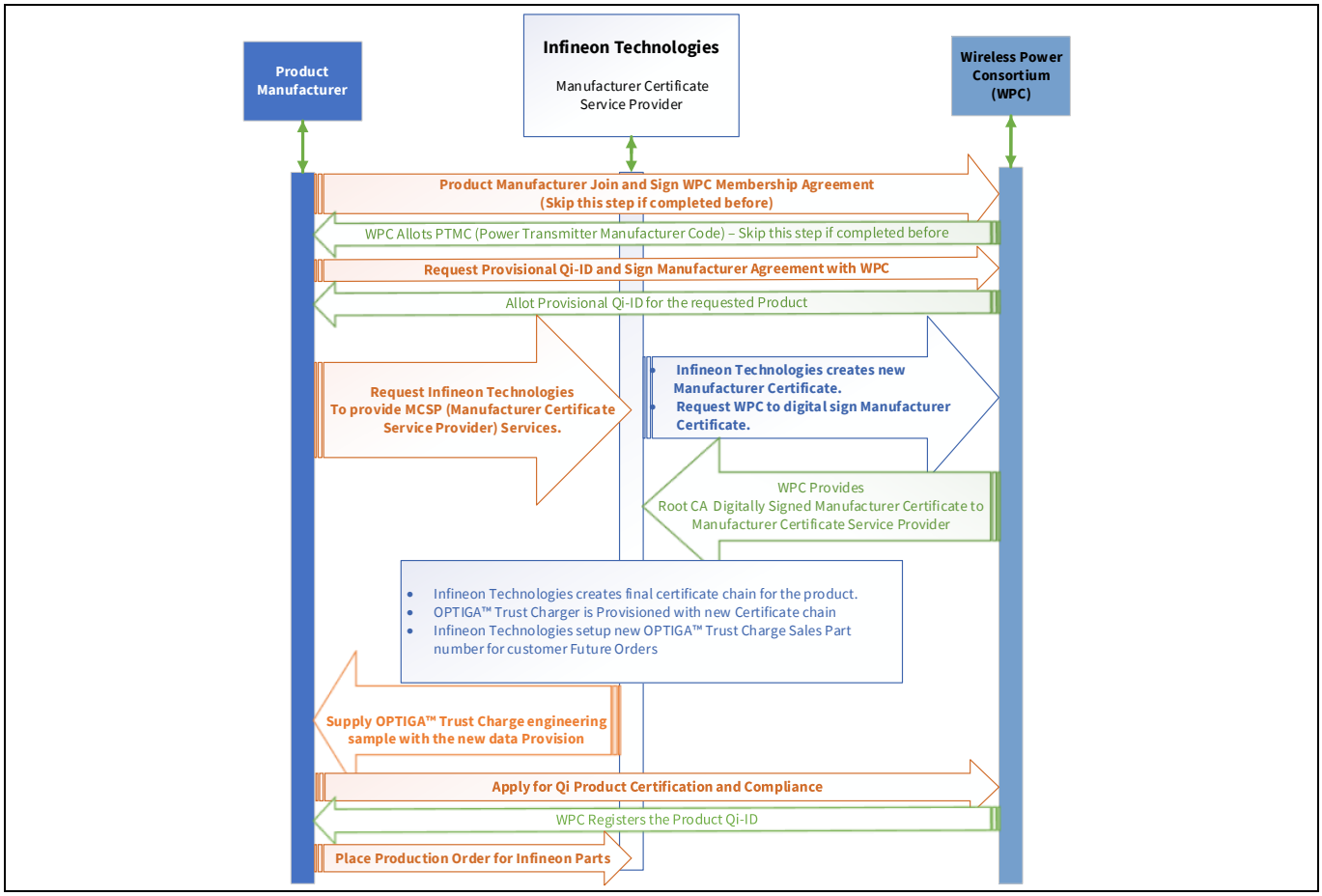

Figure 2 Process for provisioning OPTIGA™ Trust Charge

4.1 Information required in setting up certificate chain data

1. WPC membership

a) Navigate to **https://www.wirelesspowerconsortium.com/members/join-the-wpc** and fill all the required fields to create a WPC membership. WPC membership will create a power transmitter manufacturer code (PTMC).

b) Qi-ID: Reserve a Qi-ID for the new product. This process involves signing a legal agreement called "**Qi Authentication Agreement for a Manufacturer**" with WPC.

2. Fill out a standard form for assigning "Infineon Technologies" as your manufacturer CA service provider.

Note: *Infineon Technologies is one of the WPC-approved manufacturer CA service providers. Product manufacturers should contact Infineon Technologies to receive manufacturer CA service provider services.*

4.2 WPC-compliant certificate chain data

The WPC-compliant certificate chain is provisioned in OPTIGA™ Trust Charge, as shown in the following figure.

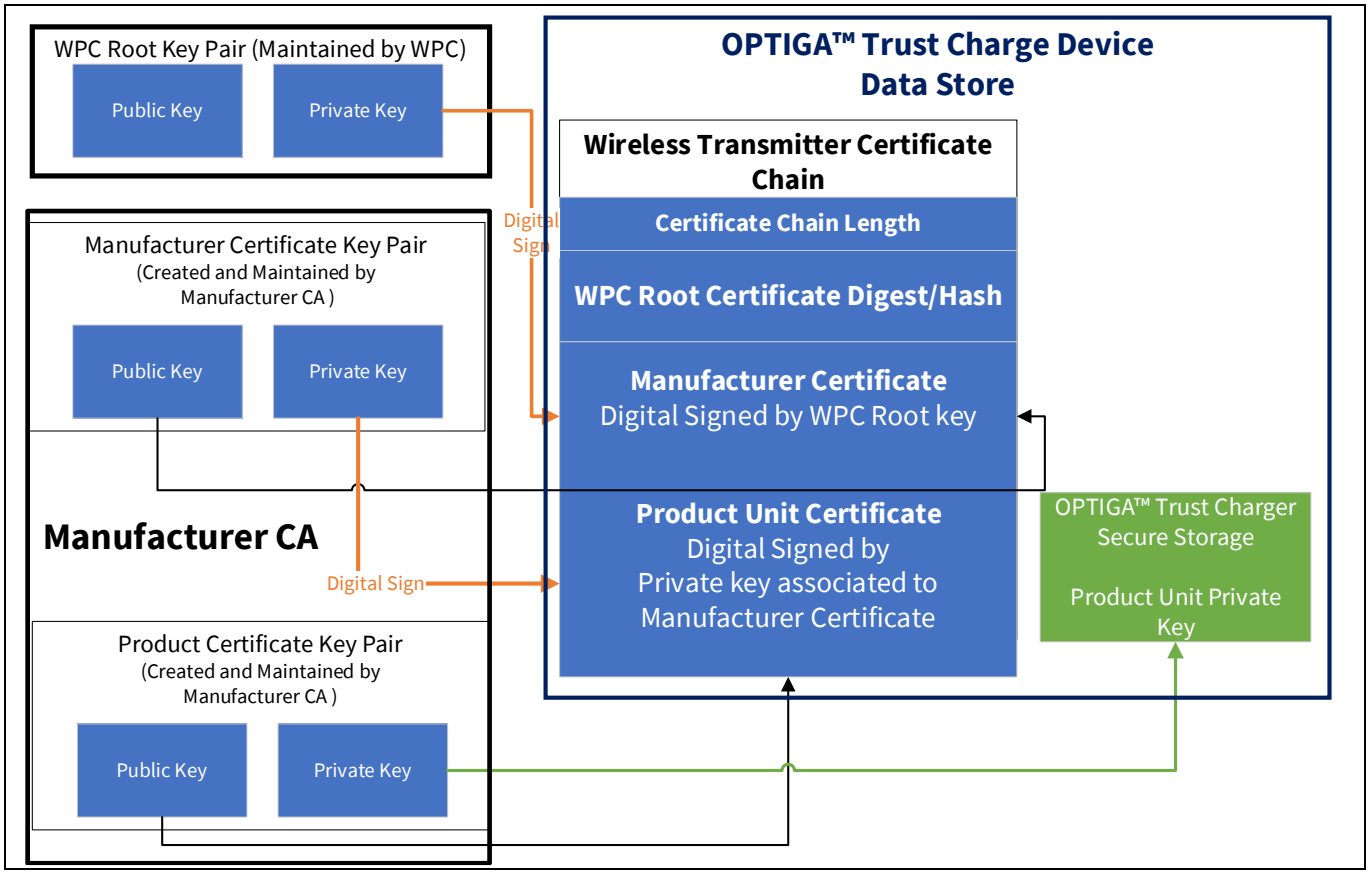

Figure 3 Certificate chain data in OPTIGA™ Trust Charge

5 WPC compliance mandate

WPC compliance in the Qi 1.3.x specification mandates the need for public key authentication for all the EPP PD of more than 5 W. Product manufacturers can benefit by reusing the reference design logo certification to achieve end-product logo compliance.

There are two possible routes:

- Substantially similar product
- Fresh product registration compliance certification

5.1 Substantially similar product

A substantially similar product is identical to a previously registered product, except for the properties that do not influence the wireless power functionality. For example, a different color, or a different brand name. Products that have different components, coils, shielding or even different metal parts in their housing do not qualify as substantially similar. The criteria for determining substantial similarity are described in “Annex D of the Wireless Power Logo License Agreement”.

5.2 Fresh product registration compliance certification

This fresh product registration process is required for those adaptations where the product manufacturer has made changes to the bill of materials (BOM) and/or for those designs that do not satisfy Annex D of the logo license agreement.

Refer to the **WPC** website for a suitable workflow option.

6 Abbreviations

Table 2 Abbreviations

Abbreviation	Definition
ASN	Abstract syntax notation
CA	Certificate authority
DER	Distinguish encoding rule
PKI	Public key infrastructure
MCSP	Manufacturer certificate service provider
WPC	Wireless Power Consortium

References

[1] **Qi 1.3.x authentication specification**

[2] **OPTIGA™ Trust Charge product datasheet and product brief**

[3] **X.509 public key infrastructure certificate**

Revision history

Document version	Date of release	Description of changes
**	2022-05-02	Initial release

Trademarks
All referenced product or service names and trademarks are the property of their respective owners.

Edition 2022-05-02

Published by

Infineon Technologies AG

81726 Munich, Germany

Do you have a question about this document?

Email: www.infineon.com/support

Document reference

002-35196 Rev. **

IMPORTANT NOTICE

The information contained in this application note is given as a hint for the implementation of the product only and shall in no event be regarded as a description or warranty of a certain functionality, condition or quality of the product. Before implementation of the product, the recipient of this application note must verify any function and other technical information given herein in the real application. Infineon Technologies hereby disclaims any and all warranties and liabilities of any kind (including without limitation warranties of non-infringement of intellectual property rights of any third party) with respect to any and all information given in this application note.

The data contained in this document is exclusively intended for technically trained staff. It is the responsibility of customer's technical departments to evaluate the suitability of the product for the intended application and the completeness of the product information given in this document with respect to such application.

For further information on the product, technology, delivery terms and conditions and prices please contact your nearest Infineon Technologies office (**www.infineon.com**).

WARNINGS

Due to technical requirements products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by Infineon Technologies in a written document signed by authorized representatives of Infineon Technologies, Infineon Technologies' products may not be used in any applications where a failure of the product or any consequences of the use thereof can reasonably be expected to result in personal injury.