

为无线充电 (WLC) 发射端配置 OPTIGA™ Trust Charge

应用笔记

关于本文档

范围和目的

本文档介绍了无线充电器 (WLC) 发射端系统的身份鉴权功能提供 OPTIGA™ Trust Charge 方案。

目标读者

在终端产品中采用 WLC 参考设计的制造商。

目录

关于本文档	1
目录	1
1 简介	2
2 采用 OPTIGA™ Trust Charge 设计的 WLC 发射端	3
3 公钥基础设施	5
4 配置 OPTIGA™ Trust Charge	6
4.1 设置证书链数据所需的信息	7
4.2 符合 WPC 的证书链数据	7
5 WPC 合规要求	8
5.1 大体相似的产品	8
5.2 新产品注册合规认证	8
6 缩略词	9
参考材料	10
文档修订记录	11
免责声明	12

简介

1 简介

本文档描述了通过使用 OPTIGA™ Trust Charge 进行 Qi 身份验证过程所需的 WLC 系统架构中的各个模块。Qi 1.3.x 规范要求对超过 5 W 的扩展电源配置文件 (EPP) 电力传输 (PD) 进行身份验证。

Qi 验证是一种建立和验证发射端身份的防篡改方法。它使接收端匹配于发射端，以在 Qi 规范的范围内运行。OPTIGA™ Trust Charge 启用 WLC 发射端的身份验证功能，从而确保 WLC 发射端系统保持符合 Qi 规范。

OPTIGA™ Trust Charge 的主要功能包括:

- 获取 Common Criteria EAL 6+认证的安全保存子系统
- 支持具有 DER 编码的 X.509 v3，用于证书格式
- 基于 ECDSA 的身份验证
- 加密算法支持: NIST P-256、SHA2
- OPTIGA™ Trust Charge 符合 WPC 规范所规定的安全和身份验证要求
- OPTIGA™ Trust Charge 方案附带了制造商证书服务提供商(MCSP)，用于创建和提供将要颁发给制造商组织的 WPC 签名证书链
 - 该过程会为客户组织创建一个新的 OPTIGA™ Trust Charge 销售器件型号

为无线充电 (WLC) 发射端配置 OPTIGA™ Trust Charge

应用笔记

采用 OPTIGA™ Trust Charge 设计的 WLC 发射端

2 采用 OPTIGA™ Trust Charge 设计的 WLC 发射端

通过 I²C 总线将 OPTIGA™ Trust Charge 与 WLC 发射端系统处理器连接，如 Figure 1 和 Figure 2 所示。WLC 发射端系统处理器具有所有硬件/固件功能，可以使用 OPTIGA™ Trust Charge 进行 Qi 身份验证功能，而无需任何补充技术条件。

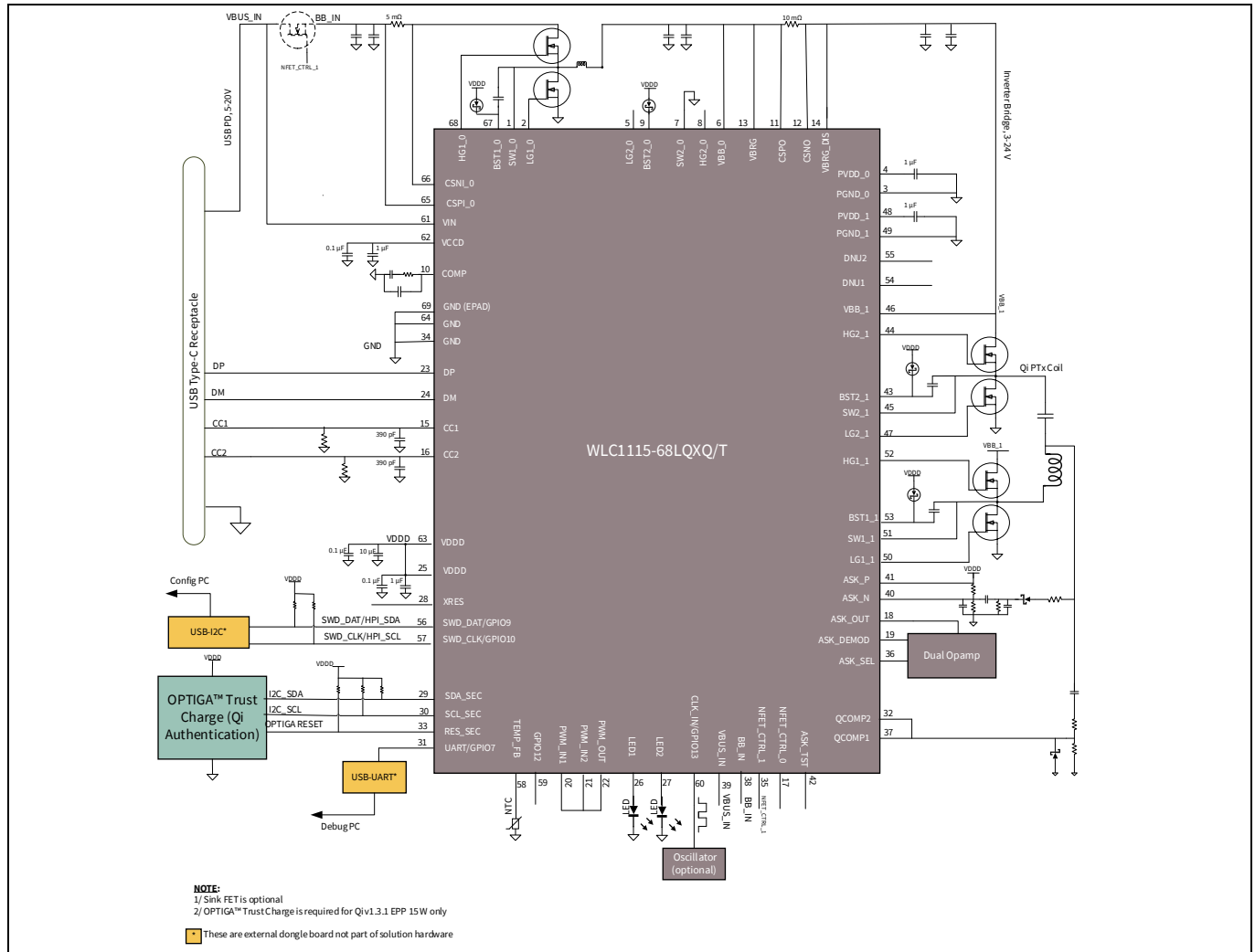


Figure 1 基于 WLC1115 的 WLC 发射端系统设计

为无线充电 (WLC) 发射端配置 OPTIGA™ Trust Charge

应用笔记

采用 OPTIGA™ Trust Charge 设计的 WLC 发射端

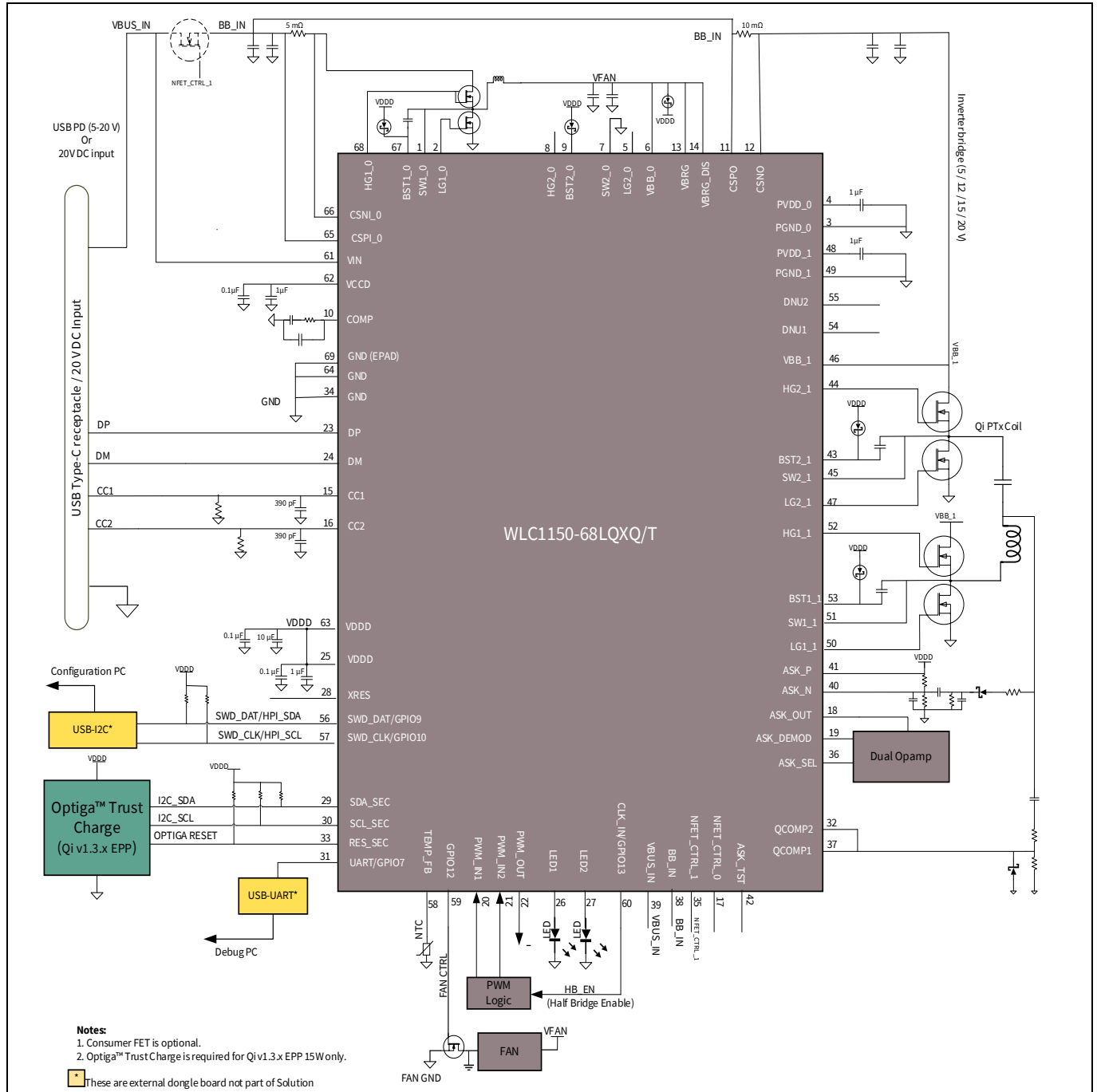


Figure 2 基于 WLC1150 的 WLC 发射端系统设计

3 公钥基础设施

Qi 规范遵循公钥基础设施 (PKI)，并在 Qi 无线充电器加密中使用以下加密方法。

Table 1 Qi 无线充电器加密方法

方法	使用情况
X.509 v3、ANS.1 DER 编码	证书格式
使用 NIST P256 和 secp256r1 曲线的 ECDSA	证书和身份验证消息的数字签名
SHA-256	Hash 算法用于 ECDSA 计算以及创建证书和证书链的摘要

WPC 公钥加密 (PKC) 依靠公钥和私钥对内容进行加密和解密。这些密钥在数学上是相关的，由其中一个密钥加密的内容可以使用另一个密钥解密。私钥是最敏感的安全凭证，必须安全存储。公钥通常是二进制证书的一部分，该证书通过通信媒介传输给接收者。

公钥证书的接收者可以执行以下操作：

- 密码验证公钥证书数据来源的真实性
- 密码验证由发射端中的“安全存储子系统”签名的随机数

X.509 PKI 标准确定了稳定的公钥证书的要求。公钥证书是一种数字签名的数据结构，它将公钥与发射端身份绑定。公钥证书由证书颁发机构 (CA) 颁发。

PKI 是用于创建、管理、分发、使用、存储和撤销数字证书所需的角色、策略、硬件、软件和程序的组合。WPC 定义了数字签名证书链创建的 PKI 流程和规则。有关详细信息，请参阅 Qi 规范和 WPC-PKI 网页中的身份验证协议手册。

为实现数字签名，Qi 规范要求发射端将产品单元的私钥安全地托管在安全存储子系统中。该私钥用于对来自发射端的随机数进行数字签名。

为无线充电 (WLC) 发射端配置 OPTIGA™ Trust Charge

应用笔记

配置 OPTIGA™ Trust Charge

4 配置 OPTIGA™ Trust Charge

WLC 发射端芯片具有两种参考设计，如 Table 2 所示。

Table 2 WLC 发射端参考设计

#	WLC 芯片 MPN	参考设计
1	WLC1115	REF_WLC_TX15W_C1
2	WLC1150	REF_WLC_TX50W_N1

WLC 发射端解决方案是制造商适配的参考设计。REF_WLC_TX15W_C1 参考设计的 OPTIGA™ Trust Charge 中的公钥证书数据包含：

- 英飞凌科技作为发射端制造商组织
- WLC 发射端解决方案参考设计的 Qi 标识证书注册 Qi-ID

Note: REF_WLC_TX50W_N1 未通过 Qi 标志认证，并使用测试证书作为演示目的。

因此，必须在 OPTIGA™ Trust Charge 中配置制造商证书数据和产品单元证书数据，以代表制造商的最终产品。以下流程图描述的是为终端制造商组织和最终产品标识注册 Qi-ID 配置 OPTIGA™ Trust Charge 所涉及的流程。该流程都适用于基于 WLC1115 和 WLC1150 的设计。

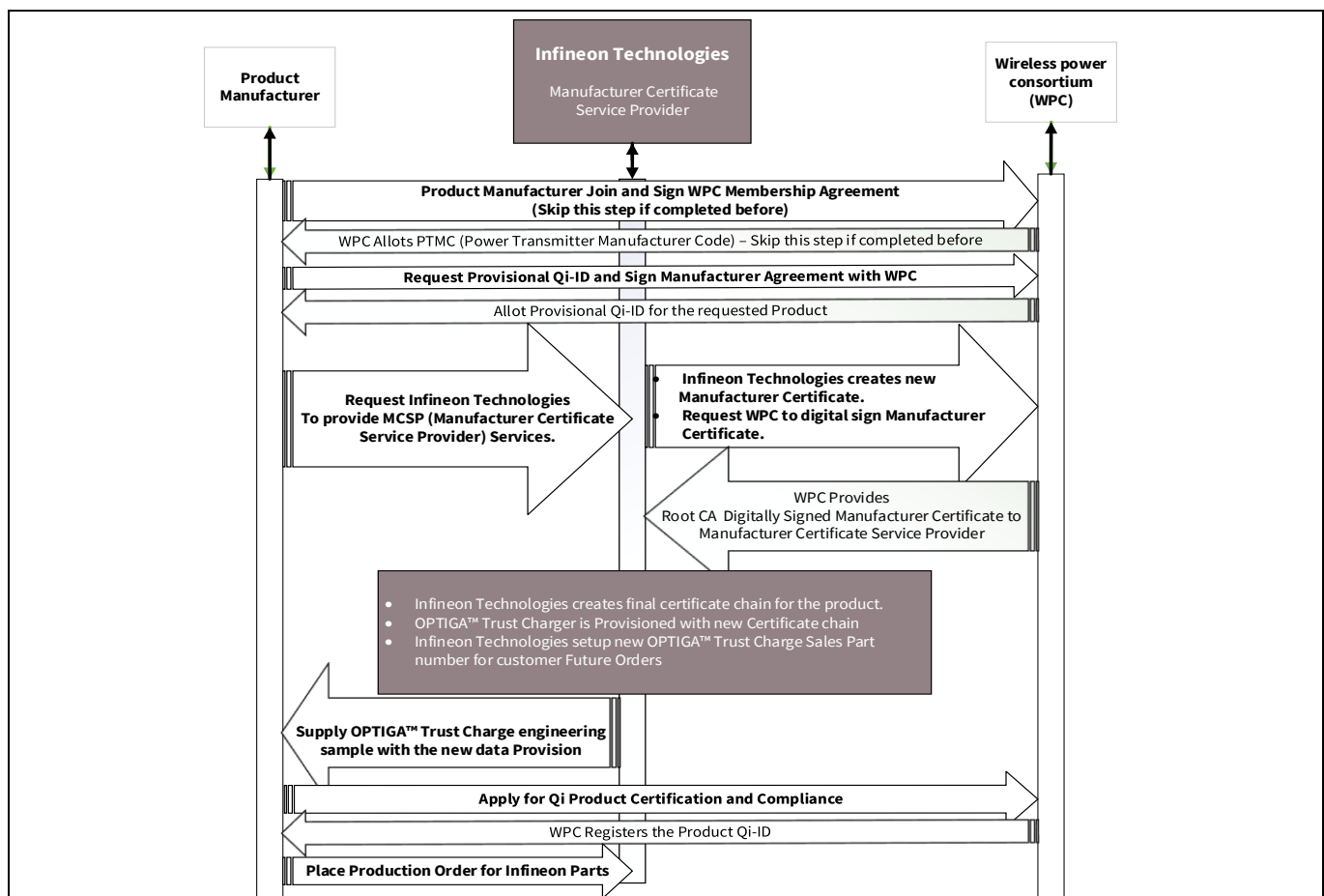


Figure 3 配置 OPTIGA™ Trust Charge 的流程

为无线充电 (WLC) 发射端配置 OPTIGA™ Trust Charge

应用笔记

配置 OPTIGA™ Trust Charge

4.1 设置证书链数据所需的信息

1. WPC 成员

- 打开[无线电力联盟](#)页面，并填写所有必填字段创建一个 WPC 会员。WPC 会员将创建一个发射端制造商代码 (PTMC)。
- Qi-ID: 为新产品预留 Qi-ID。该流程包括与 WPC 签署名为“[Qi 制造商身份验证协议](#)”的法律协议。

2. 请填写标准表格，将“Infineon Technologies”指定为您的制造商 CA 服务提供商。

Note: 英飞凌科技是 WPC 批准的制造商 CA 服务提供商之一。制造商应联系英飞凌科技以获得制造商 CA 服务供应商的服务。

4.2 符合 WPC 的证书链数据

符合 WPC 的证书链在 OPTIGA™ Trust Charge 中提供，如下图所示。

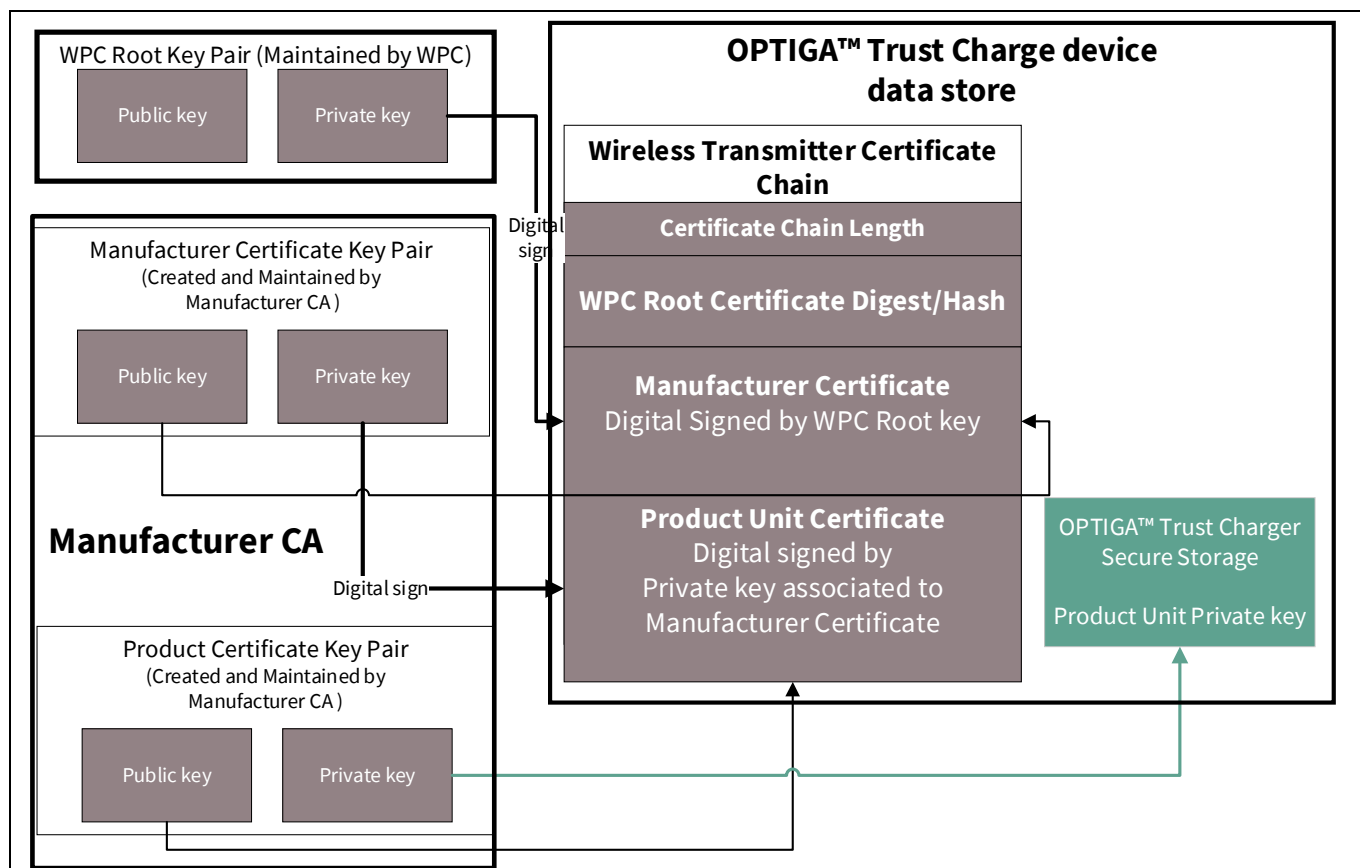


Figure 4 OPTIGA™ Trust Charge 中的证书链数据

5 WPC 合规要求

Qi 1.3.x 规范中的 WPC 合规性要求对所有超过 5 W 的 EPP PD 进行公钥认证。制造商可以受益于重复使用参考设计标识认证来实现最终产品标识合规性。

有两种可能的路线:

- 大体相似的产品
- 新产品注册合规认证

5.1 大体相似的产品

除了不影响无线电力功能的特性外，大体相似的产品与先前注册的产品完全相同。例如，不同的颜色或不同的品牌名称。外壳中带有不同组件、线圈、屏蔽甚至不同金属部件的产品不符合实质性相似的条件。确定大体相似的标准如“无线电力标识许可协议的附件 D”中所述。

5.2 新产品注册合规认证

对于制造商对材料清单 (BOM) 进行更改和/或不满足标识许可协议附件 D 的设计，则需要进行新产品注册流程。

请参阅 [WPC](#) 网站，了解合适的工作流程选项。

6 缩略词

Table 3 缩略词

缩略词	定义
ASN	抽象语法符号
CA	证书颁发机构
DER	区分编码规则
PKI	公钥基础设施
MCSP	制造商证书服务提供商
WPC	无线电力联盟

参考材料

- [1] [Qi 1.3.x 身份验证规范](#)
- [2] [OPTIGA™ Trust Charge 产品数据手册和产品简介](#)
- [3] [X.509 公钥基础设施证书](#)

为无线充电 (WLC) 发射端配置 OPTIGA™ Trust Charg

应用笔记

文档修订记录

文档修订记录

版本	提交日期	变更说明
**	2022-06-17	翻译自: 002-35196 Rev. **
*A	2023-03-22	翻译自: 002-35196 Rev. *A

Trademarks

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

Edition 2023-03-22

Published by

Infineon Technologies AG

81726 Munich, Germany

© 2023 Infineon Technologies AG.

All Rights Reserved.

Do you have a question about this document?

Go to www.infineon.com/support

Document reference

002-35681 Rev. *A

重要提示

本文档所提供的任何信息**绝不当**被视为针对任何条件或者品质而做出的**保证**（质量保证）。英飞凌对于本文档中所提及的任何事例、提示或者任何特定数值及/或任何关于产品应用方面的信息均在此明确声明其不承担任何保证或者责任，包括但不限于其不侵犯任何第三方知识产权的保证均在此排除。

此外，本文档所提供的任何信息均取决于客户履行本文档所载明的义务和客户遵守适用于客户产品以及与客户对于英飞凌产品的应用所相关的任何法律要求、规范和标准。

本文档所含的数据仅供经过专业技术培训的人员使用。客户自身的技术部门有义务对于产品是否适宜于其预期的应用和针对该等应用而言本文档中所提供的信息是否充分自行予以评估。

警告事项

由于技术所需产品可能含有危险物质。如需了解该等物质的类型，请向离您最近的英飞凌科技办公室接洽。

除非由经英飞凌科技授权代表签署的书面文件中做出另行明确批准的情况外，英飞凌科技的产品不当被用于任何一项一旦产品失效或者产品使用的后果可被合理地预料到可能导致人身伤害的任何应用领域。