如何确保 Qi®无线充电的安全性？

Microchip Technology Inc.
安全与计算事业部
产品营销经理 Xavier Bignalet

WPC Qi®无线充电标准的最新更新增加了安全身份验证，确保支持 Qi 的设备和充电器可以安全地协同工作。

过去几年中，无线充电联盟（WPC）一直在忙于以多种方式更新广泛采用的 Qi 标准。当然，随着世界的互联互通变得越来越普遍，无线充电的安全性始终是首要考虑的问题。Qi 无线充电规范的版本 1.3 增加了安全身份验证功能。

版本 1.3 允许支持 Qi 的设备验证充电器的身份及其对 Qi 规范的遵守情况（图 1）。这样便可确定充电器与 Qi 标准是否兼容，以确保它不会损坏或破坏正在充电的产品。它本质上是 Qi 版本 1.2 的扩展，但增加了一层保护（身份验证），以确保手机和充电器可以协同工作。Qi 1.3 定义了两种功率配置，基准功率配置可以提供最高 5W 的输出，而扩展功率配置则可将输出增加到 15W。

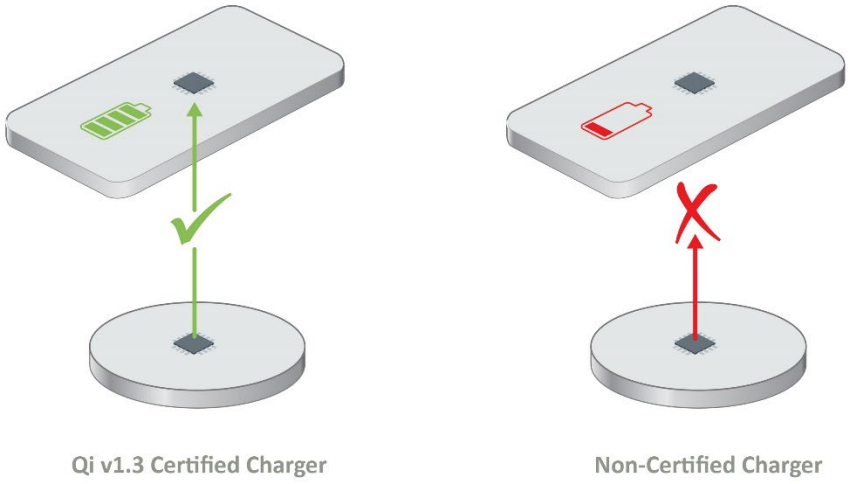

图 1.通过 CryptoAuthLib 进行单向身份验证

简单来说，在充电开始之前，要充电的设备（通常是智能手机）确认它正在与一台通过 Qi 认证的充电设备进行交互。举例来说，如果是智能手机，则会请求最适当和最安全的充电功率。如果身份验证失败，手机将取消请求或者充电器将其输出功率降低到 5W（基准）。

为了实现身份验证，充电器制造商必须在其产品中包含称为“产品单元证书”的公钥基础架构（PKI）。这种关键功能的实现方式为，创建一个位于嵌入在充电器中单片机旁边的安全元

件来存储关键信息（图 2）。PKI 是一种用于提供身份验证的超可靠技术，因为它使用自己的专用处理器和存储器，而不是共享资源，从而降低了安全风险。

图 2.Qi 1.3 标准要求必须进行安全配置

安全元件的概念已经在许多应用中使用了超过 15 年，而且信用卡、智能支付系统和加密货币交易服务器中也在广泛采用。如今，每台智能手机制造商都使用安全元件。

安全的身份验证涉及安全的生产流程，并结合采用可形成安全存储子系统（SSS）（通常称为安全密钥存储器件或安全元件）的过程。手机将要求充电器提供证书和签名，以验证其为具有私钥的 WPC 认证产品，并签署由手机发出的质询，证明其已获知机密信息且不曾泄露。Qi 1.3 标准要求私钥必须由经过认证的 SSS 存储和保护。椭圆曲线数字签名算法和私钥都必须处于同一位置，以确保它在身份验证中的信任级别。

SSS 必须根据通用标准联合解析库（JIL）漏洞评分系统证明其保护加密密钥的稳健性，该系统于 21 世纪中期首次推出，用于提高智能卡的效率和安全性。现在，它已成为其他许多需要安全功能的应用的稳健基准。

制造充电器时，还需要其他步骤来保护信任级别，目标是消除对私钥的暴露。要构建这种可信链，所有私钥都必须位于生产场地的硬件安全模块（HSM）中或充电器的 SSS 内。然后，必须确定这些私钥的产生、存储和构成可信链的方式，这些流程通过密钥仪式实现。完成后，现已通过加密方式建立了可信链，同时不会暴露给外部合约制造商或第三方。结果，WPC、手机和充电器之间建立了信任。

WPC 建立的认证过程相当复杂，对充电器制造商提出了挑战，但那些在合规方面具有丰富专业知识的制造商除外。由于单片机是执行所有必要合规操作步骤的组件，因此如果设计人员直接与单片机制造商合作，认证过程可以大大简化。

例如，Microchip 是率先将此过程中所有要素结合起来的公司之一，它利用其“可信平台”完成公司安全元件的初始配置，帮助设计人员完成各种步骤，而无需依赖多个来源。

Microchip 是一家获得 WPC 许可的制造证书颁发机构，可提供预配置的安全存储子系统解决方案，能够借助 WPC 根证书颁发机构来处理整个密钥仪式。它提供了一种认证参考设计，包括 MCU、Qi 1.3 软件协议栈、具有支持加密库的 SSS 以及面向汽车和消费者应用的配置服务。利用公司安装在 Microchip 工厂内的 HSM，可在每个安全元件的边界内生成凭证。

迈向 Qi 版本 2

WPC 的下一步是实施 Qi 版本 2 标准，预计将于今年晚些时候推出。它将使 Qi 充电的方式更加多样化，同时保留 Qi 1.3 建立的所有关键安全功能。

Qi 无线充电标准已经建立起极高的安全级别，而且还在不断改进以满足更多类型设备的需求，特别是那些由于外形导致其出色功能无法被触及的设备。