Qi 充電獲得亟需的安全效能提升

2021 年發佈的 Qi 1.3 標準在確保提高充電器對消費者的安全性方面發揮了很大作用。

■作者：Xavier Bignalet / Microchip 安全產品部產品行銷經理

新技術的出現受到了反對意見的阻礙，Qi 感應式充電技術頗費時日才被廣泛接受。因此，雖然 Qi 早在 2010 年就已發佈，但又過了五年才佔據主導地位。自那時起，無線充電聯盟 (WPC) 對 Qi 進行了重大改進，但直到 2021 年初，聯盟才增加了一項協定，使支援 Qi 的設備製造商能夠驗證充電器的身份及其對 Qi 規範的遵守情況。這項功能可以剔除那些可能損害甚至損毀其充電產品的充電器，因此無疑是 Qi 1.3 中最重要的新特性。

具體來說，Qi 1.3 規範要求充電器製造商必須在無線充電器中嵌入稱為“產品單元證書”的公開金鑰基礎架構 (PKI)，以使其能夠對智慧手機進行身份驗證。該關鍵功能透過嵌入式方式實現，因為它採用最穩健但最基礎的方法 — 由安全元件構成與微控制器相鄰的保險金庫，將關鍵資訊與設備的主處理器 (圖 1) 隔離儲存。此功能將使得規避安全機制變得極端困難，並且可以使用自己專用的獨立處理能力和記憶體，無需任何共用資源。

安全元件並非新鮮事物，它已在物聯網、信用卡、支付系統和加密貨幣交易等領域廣泛應用。例如，自 2009 年以來，現在廣泛用於智慧支付的 NFC 一直依賴安全元件，從 2019 年起，幾乎所有智慧手機都整合了安全元件，因此，將這項技術添加到無線充電中並不算為時過早。

圖 1：Qi 1.3 標準要求必須進行安全配置

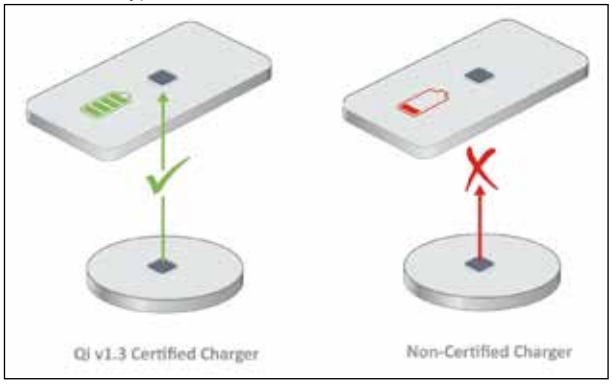
工作原理

身份驗證過程比較複雜，但此過程是在後臺進行的，不需要人為干預且用時不到一秒。手機是接收器，它位於充電器 (在規範中被稱為發射器) 上。Qi 1.3 規定必須進行單向身份驗證，這意味著發射器必須以加密方式向手機證明其可信且被識別為 WPC 生態系統的安全成員 (圖 2)。

如果沒有經過身份驗證，手機可以完全拒絕充電，更典型的情況是將接受的充電功率限制在 5W 而不是 15W，從而導致充電緩慢。由於大多數智慧手機同時運行多個應用程式，造成的結果是用戶體驗不佳，進而會對充電器製造商的聲譽產生負面影響。

要實現高效、安全的身份驗證，還必須採用安

圖 2：透過 CryptoAuthLib 進行單向身份驗證



全的生產流程，並結合採用可形成安全儲存子系統 (SSS) (通常稱為安全金鑰記憶體件或安全元件) 的過程。Qi 1.3 使用從充電器到手機的單向身份驗證，在此期間，充電器必須以加密方式向手機證明其可信。如果身份驗證失敗，手機有兩個選擇：它可以將充電功率從最大 15W 降低到 5W，或者拒絕充電器。

如果更深入地研究該過程，手機將要求充電器提供證書和簽名，以驗證其為具有私密金鑰的 WPC 認證產品，並簽署由手機發出的質詢，證明其已獲知機密資訊且不曾洩露。Qi 1.3 標準要求私密金鑰必須由經過認證的 SSS 儲存和保護。橢圓曲線數位簽章演算法和私密金鑰都必須在同一實體安全邊界內，以確保可信的身份驗證。

SSS 必須根據 Joint Interpretation Library (JIL) 漏洞評分系統證明其保護加密金鑰的穩健性，該系統於 2000 年代中期首次推出，用於提高智慧卡的效率和安全性，現已成為其他許多需要安全功能的應用的穩健基準。它側重於評估安全元件的儲存強度，以確定其達到的特定 JIL 級別，JIL 從五個方面對效能進行評級：

■破解演算法所需的時長
■攻擊者必須具備的技能水準
■要實現成功的攻擊需要對評估物件 (TOE) 的瞭解程度 (在此種情況下，TOE 是指充電器)
■獲得 TOE 樣本所需的難度，以及需要的樣本數
■一次成功攻擊需要何種類型的設備

在充電器可供銷售之前，需要採取其他步驟來保護充電器在生產時所具備的信任級別，目的是消除對私密金鑰的暴露。要構建可信鏈，所有私密金鑰都必須位於生產場地的硬體安全模組 (HSM) 中或充電器的 SSS 內。然後，必須確定這些私密金鑰的產生、儲存和構成可信鏈的方式。這是透過 WPC 所謂的金鑰儀式實現的。完成後，現已透過加密方式建立了可信鏈，同時不會暴露給外部合約製造商或協力廠商。結果是，WPC、手機和充電器三者之間相互信任，這意味著 WPC 可以信任手機，反之亦然。

認證生態系統

由於可信鏈需要各方的參與，因此認證過程對參與其中的各方來說都是十分艱巨的任務，從微控制器製造商到充電器本身的製造商，均是如此。為了解決這一問題，Microchip 是率先將這一過程的所有要素結合起來的公司之一，其目的在協助設計人員開發產品，同時無需承擔必須依賴多個來源的艱巨任務。Microchip 採取的方法是透過可信平臺提供公司安全元件的初始配置，以加快產品的上市時間。

Microchip 是一家獲得 WPC 許可的製造憑證授權商，可提供預配置的安全儲存子系統解決方案，以降低複雜性並縮短開發時間。此外，透過由 WPC 根憑證授權來處理整個金鑰儀式，技術門檻也得到降低。作為完整的認證參考設計，可信平臺包括應用 MCU、Qi 1.3 軟體協定堆疊、具有支援加密庫的安全儲存子系統，以及面向汽車和消費性應用的配置服務。

可信平臺包含一系列預先配置或完全可客製化的安全元件。透過利用公司安裝在 Microchip 工廠內的硬體安全模組 (HSM)，可在每個安全元件的邊界內生成憑證。這些元件還配備了硬體和軟體發展工具，可輕鬆進行原型設計並快速進行設計開發。

總結

對於像充電器這樣看似簡單的設備來說，這一切似乎有點誇張，但市場上充斥著數百種不同的充電器，在 Qi 1.3 之前，從來沒有一種有效的方法可以驗證它們是優質產品還是劣質產品，後者不僅可能損壞目標設備 (智慧手機)，還可能引發更糟糕的結果。例如，如果充電器安裝在車輛中，不當操作不僅會影響智慧手機，還會影響車輛本身的某些部分。這種等級的安全性期待已久，但它終究對所有人有所助益，尤其是廣大消費者。 CTA