

Qi 無線充電安全性須知

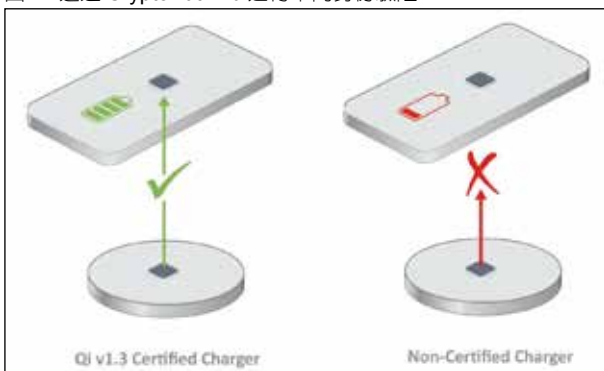
WPC Qi 無線充電標準的最新更新增加了安全身份驗證，確保支援 Qi 的設備和充電器可以安全地協同工作。

■作者：Xavier Bignalet
Microchip 安全與計算事業部產品行銷經理

過去幾年中，無線充電聯盟 (WPC) 一直在忙於以多種方式更新廣泛採用的 Qi 標準。當然，隨著世界的互聯互通變得越來越普遍，無線充電的安全性始終是首要考慮的問題。Qi 無線充電規範的版本 1.3 增加了安全身份驗證功能。

版本 1.3 允許支援 Qi 的設備驗證充電器的身份及其對 Qi 規範的遵守情況 (圖 1)。這樣便可確定充電器與 Qi 標準是否相容，以確保它不會損壞或破壞正在充電的產品。它本質上是 Qi 版本 1.2 的擴展，但增加了一層保護 (身份驗證)，以確保手機和充電器可以協同工作。Qi 1.3 定義了兩種功率配置，基準功率配置可以提供最高 5W 的輸出，而擴展功率配置則可將輸出增加到 15W。

圖 1：透過 CryptoAuthLib 進行單向身份驗證



簡單來說，在充電開始之前，要充電的設備 (通常是智慧手機) 確認它正在與一台透過 Qi 認證的充電設備進行互動。舉例來說，如果是智慧手機，則會請求最適當和最安全的充電功率。如果身份驗證失敗，手機將取消請求或者充電器將其輸出功率降低到 5W (基準)。

為了實現身份驗證，充電器製造商必須在其產品中包含稱為“產品單元證書 (Product Unit Certificates)”的公開金鑰基礎架構 (PKI)。這種關鍵功能的實現方式為，創建一個位於嵌入在充電器中微控制器旁邊的安全元件來儲存關鍵資訊 (圖 2)。PKI 是一種用於提供身份驗證的超可靠技術，因為它使用自己的專用處理器和記憶體，而不是共用資源，因而降低了安全風險。

圖 2：Qi 1.3 標準要求必須進行安全配置



安全元件的概念已經在許多應用中使用了超過 15 年，而且信用卡、智慧支付系統和加密貨幣交易伺服器中也在廣泛採用。如今，每台智慧手機製造商都使用安全元件。

安全的身份驗證涉及安全的生產流程，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。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認證要求，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 (Elliptic Curve Digital Signature Algorithm) 和私密金鑰都必須處於同一位置，以確保它在身份驗證中的信任級別。

SSS 必須根據通用標準聯合解析庫 (JIL) 漏洞評分系統證明其保護加密金鑰的穩健性，該系統於 21 世紀中期首次推出，用於提高智慧卡的效率和安全性。現在，它已成為其他許多需要安全功能的應用的堅實標準。

製造充電器時，還需要其他步驟來保護信任級別，目標是消除對私密金鑰的暴露。要構建這種可信鏈，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，這些流程通過金鑰儀式實現。完成後，現已通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，WPC、手機和充電器之間建立了信任。

WPC 建立的認證過程相當複雜，對充電器製造商提出了挑戰，但那些在合規方面具有豐富專業知識的製造商除外。由於微控制器是執行所有必要合規操作步驟的元件，因此如果設計人員直接與微控制器製造商合作，認證過程可以大大簡化。


例如，Microchip 是率先將此過程中所有要素

結合起來的公司之一，它利用其“可信平臺”完成公司安全元件的初始配置，協助設計人員完成各種步驟，而無需依賴多個來源。

Microchip 是一家獲得 WPC 許可的製造憑證授權，可提供預配置的安全儲存子系統解決方案，能夠借助 WPC 根憑證授權來處理整個金鑰儀式。它提供了一種認證參考設計，包括 MCU、Qi 1.3 軟體協定堆疊、具有支援加密庫的 SSS 以及面向汽車和消費性應用的配置服務。利用公司安裝在 Microchip 工廠內的 HSM，可在每個安全元件的邊界內生成憑證。

邁向 Qi 版本 2

WPC 的下一步是實施 Qi 版本 2 標準，預計將於今年晚些時候推出。它將使 Qi 充電的方式更加多樣化，同時保留 Qi 1.3 建立的所有關鍵安全功能。

Qi 無線充電標準已經建立起極高的安全級別，而且還在不斷改進以滿足更多類型設備的需求，特別是那些由於外形導致其出色功能無法被觸及的設備。 

Microchip 推出 PIC18-Q24 系列微控制器，為增強程式安全性設置新標準

從手機、汽車到智慧恆溫器和家用電器，越來越多日常設備與雲端相連。隨著連線性增多，在晶片層面部署先進的安全措施以保護韌體和資料，就變得至關重要。為了應對當前和不斷擴大的安全威脅，Microchip 發佈 PIC18-Q24 系列微控制器 (MCU)。

為應對在嵌入式系統中對元件進行惡意竄改程式的威脅，PIC18-Q24 微控制器引入了程式設計和除錯介面禁用 (PDID) 功能。啟用後，這一增強型程式碼保護功能將鎖定對程式設計 / 除錯介面的存取，並阻止未經授權的讀取、修改或抹除韌體的嘗試。

由於許多安全系統經常與各種感測器、儲存晶片和處理器連接和通訊，因此 PIC18-Q24 系列微控制器具有多電壓 I/O (MVIO) 功能。該功能無需使用外部電位轉換器，使微控制器能以不同工作電壓連接數位輸入或輸出。除了降低電路板複雜性和物料清單 (BOM) 成本外，MVIO 功能還使 PIC18-Q24 系列微控制器特別適合作系統管理處理器，為大型處理器執行監控和遙測任務。嵌入式系統中這些看似常規的任務通常最容易受到潛在駭客的攻擊。

PIC18-Q24 系列微控制器還提供不可更改的開機載入程式 (bootloader) 選項，適用於需要安全升級韌體的應用。

PIC18-Q24 系列微控制器由 Microchip 開發生態系統提供全面支援，可與 MPLAB 程式碼配置器 (MCC) 整合設計。PIC18F56Q24 Curiosity Nano 評估工具套件 (EV01E86A) 為使用 PIC18-Q24 系列進行設計提供全面支援。

