作者：顏睿余
Microchip 應用工程師

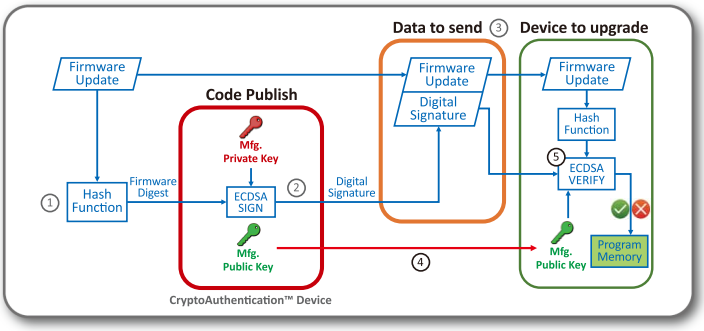
小百科

非對稱式 Security Boot/Security Update 的實作

Security Boot 是一種用於確保系統內運作的應用程式碼被授權的方法，通常由設計與構建系統的廠商提供。通過確保應用程式碼為正確的授權版本可以防止不可預測的系統程式造成機器性能異常、安全性受損甚至財產損失。大多數電子系統使用可編程非揮發性存儲器 (Flash) 存放其應用程式碼 (Application Code)，無論大小都可以利用 Security Boot 保護該程式碼不被惡意竄改。本文說明 Security Boot 的基本觀念，同時深入地介紹其處理方式並提供解決方案。

Security Update 流程

前置作業：下圖紅色方框所代表的角色為程式碼簽發者 (Code Publish)，其包含一組唯一的公鑰 (Public Key) 和私鑰 (Private Key)



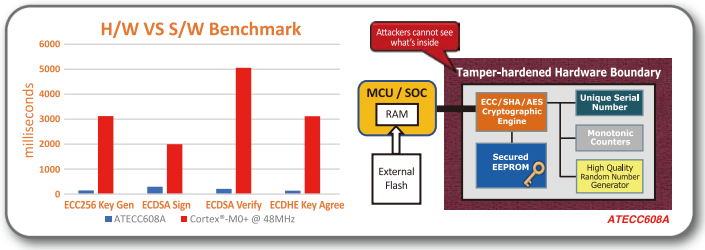
1. 要進行升級的應用程式 (Firmware update) 應該要先透過 Hash Function (例如 SHA256) 獲取其 Digest (此步驟就如同用 XOR 計算出程式碼的 Checksum，只是 SHA256 Digest 為 256-bit 遠大於 Checksum，具有絕對唯一性)。
2. 接著程式碼的簽發機構 (Code Publish) 需要針對該程式碼的 Digest 透過其私鑰進行“加密”(ECDSA SIGN)，加密過後的資料我們稱作數位簽章 (Digital Signature)。因為擁有該私鑰即擁有權力簽發正式版本程式碼的數位簽章，故一般而言私鑰將會被存放於硬體保護的晶片裡 (如 ATECC608A)，避免對外流傳。
3. 將更新應用程式與數位簽章 (Data to Send) 透過有線或是無線的方式傳送至待更新的裝置 (Device to Upgrade)。進行更新之前，待更新裝置必須驗證此應用程式與數位簽章的正確性。
4. 在非對稱的算法中，每個存在的私鑰會有一個相對的公鑰存在，其私鑰用來“加密”(ECDSA SIGN)，公鑰則用來“解密”(ECDSA VERIFY)，故更新裝置中應該要預先配備相對的公鑰。為了能限制僅搭配特定的程式碼簽發機構 (Code Publish) 作“解密”，其公鑰必須存放在一次性燒錄的記憶體中 (OTP)，避免被更換為駭客私鑰的對應公鑰。
5. 更新裝置 (Device to Upgrade) 在收到更新程式 (Firmware update) 後即先透過 Hash function (例如 SHA256) 獲取其 Digest (如同第 1 步驟)，為確認該 Digest 是否正確，必須透過公鑰對同步收到的數位簽章作解密並判斷是否符合更新程式的 Digest (ECDSA VERIFY)。若是符合，則該更新程式允以更新該裝置。反之，假設該更新程式並非官方發行程式碼 (沒有透過 Code Publish 簽發數位簽章)，經過第 5 步驟的驗證，因為其計算出來的 Digest 將不同於透過公鑰所解密的數位簽章，該程式碼則不予運作。

Security Boot 流程

如同 Security Update 流程第 5 步驟，開機後即先透過 Hash Function (例如 SHA256) 計算應用程式之 Digest，接著確認該 Digest 是否正確：透過公鑰對數位簽章作解密並判斷是否符合該應用程式的 Digest (ECDSA VERIFY)。

運行 Security Update 之裝置需求

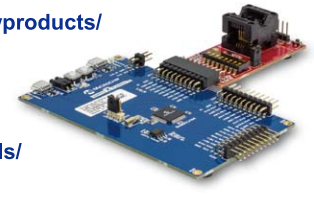
1. **一次性燒錄的記憶體**
   為了能夠完成 Security Update/Security Boot 流程，其中步驟 4 提到裝置必須預先配備公鑰於一次性燒錄的記憶體中 (OTP)，目前市售 MCU 提供 OTP 功能的並不多，或者價錢相對不便宜。
2. **進行 ECDSA VERIFY 運算**
   步驟 5 中提到需要對應用程式 Digest 與程式碼數位簽章利用 OTP 區的公鑰進行 ECDSA VERIFY 運算。該運算量相當龐大，如下圖若以 Cortex®-M0+ 進行運算將耗費 5 秒。開機若需要耗費如此多的時間將不容易被使用者接受。



Microchip 提供 ATECC608A 可外掛支援 Security Boot 功能

ATECC608A 提供基於硬體的密鑰儲存與加密算法加速器，用以實現各種身分驗證和加密協議，基於落實 Security Boot。使用者能預先將公鑰存放於 ATECC608A 的 Secured EEPROM 中，並透過 ECDSA 硬體加速器進行 Digest 和數位簽章的驗證運算 (Verify)。而運算結果亦可以透過輸出保護密鑰 (IO Protection Key) 輸出，駭客無法判讀或進行複製。相關產品資訊請參考官方網站：

- **ATECC608A 產品頁面**
  https://www.microchip.com/wwwproducts/en/atecc608a
- **ATECC608A 開發工具**
  https://www.microchip.com/DevelopmentTools/ProductDetails/DM320109



聯繫信息 > Microchip 台灣分公司
電郵：rtc.taipei@microchip.com　　技術支援專線：0800-717-718
聯絡電話：• 新竹 (03) 577-8366　• 高雄 (07) 213-7830　• 台北 (02) 2508-8600