面向配件生態系統和一次性用品應用的高性價比安全身分驗證解決方案

Microchip Technology Inc.
Xavier Bignalet

如果您對單個配件的身分驗證、規範化電子配件生態系統的構建或一次性用品的假冒偽劣處理感興趣，歡迎繼續閱讀。本篇文章將介紹我們新推出的高性價比安全身分驗證 IC 提供了哪些安全功能來協助您的安全威脅模型達成目標。

面向一次性用品和配件生態系統的成本優化型安全身分驗證 IC

不知您是否有注意到，其實我們每天都在經歷著各種安全身分驗證過程。例如，當您發送電子郵件、將手機插入充電器或列印文件時，後臺都在進行身分驗證。

本篇文章將介紹我們推出的高性價比安全身分驗證 IC 提供了哪些有價值的安全功能來協助您的安全威脅模型達成目標。

為什麼需要對配件/一次性用品進行身分驗證？

對於一次性用品和配件生態系統而言，身分驗證之所以至關重要，有幾點原因值得注意。第一點是安全性——儘管系統元件有時可能會運行比較危險的功能，但身分驗證可以證明系統是正品，確保安全工作。第二點是互通性。生態系統之所以能夠正常工作離不

開內部各元件之間的相互通信。有鑒於此，非常需要透過身分驗證來對生態系統進行控制。這樣一來，無論您的系統內的各個元件採用自家品牌還是協力廠商產品，都能夠保證為用戶提供一致的使用體驗。近年來，日漸猖獗的假冒偽劣產品亟需加強防範，系統中需要引入驗證機制，這是第三點。第四點是上面提到的用戶體驗。您可以透過韌體中的 IP 為每位用戶提供持續的獨特體驗。以上四點對於提高業績和品牌聲譽都將大有幫助。

配件/一次性用品的細分市場

配件/一次性用品技術覆蓋多個細分市場。在醫療細分市場，這類產品包括線纜、呼吸管、感測器、墨水匣和貼片等。在消費者細分市場，這類產品包括化妝品、電子煙和印刷產品，以及香薰和 Qi® 1.3 無線充電，後兩項也是汽車細分市場的常見產品。在汽車細分市場，這類產品還包括原始設備製造商（OEM）或協力廠商電子卡和電動車電池。在工業細分市場，這類產品包括協力廠商配件、維護服務和 OEM 生態系統控制。在電動車細分市場，這類產品包括電動自行車電子卡、電池更換和電池身分驗證。在資料中心細分市場，這類產品包括與 OEM 或協力廠商卡身分驗證相關的技術，用於對製造環節進行加密控制。配件/一次性用品生態系統真可謂無處不在，我們必須針對所有細分市場的產品提供身分驗證解決方案。

高階產品組合

我們的身分驗證產品組合中包含多款高階安全產品。在我們的晶片產品中，我們提供了 CryptoAuthentication™（ATECC608）元件、CryptoAutomotive™（TA100）安全 IC、可信平臺模組（TPM）（ATTPM20P）和 Platform Root of Trust。對於導入過程，我們提供了可信平臺，其中包括 Trust&GO、TrustFLEX 和 TrustCUSTOM。透過這三個安全元件，您可以利用 Microchip 安全配置服務來選擇所需的安全身分驗證 IC、想要配置的憑據，以及最適合您需求的最小起訂量（MOQ）。該平臺將全程陪伴您完成從原型設計到生產的整個過程。

安全身分驗證的工作原理

安全身分驗證 IC 可用作任何微控制器（MCU）的配套元件。其作用類似於一個保管機密資訊的保險庫。

機密資訊（金鑰、憑證和資料）在 Microchip 安全工廠內生產元件期間被配置到元件的安全邊界內。這些機密資訊受保護，不會暴露，並由 Microchip 的安全配置過程進行管理。

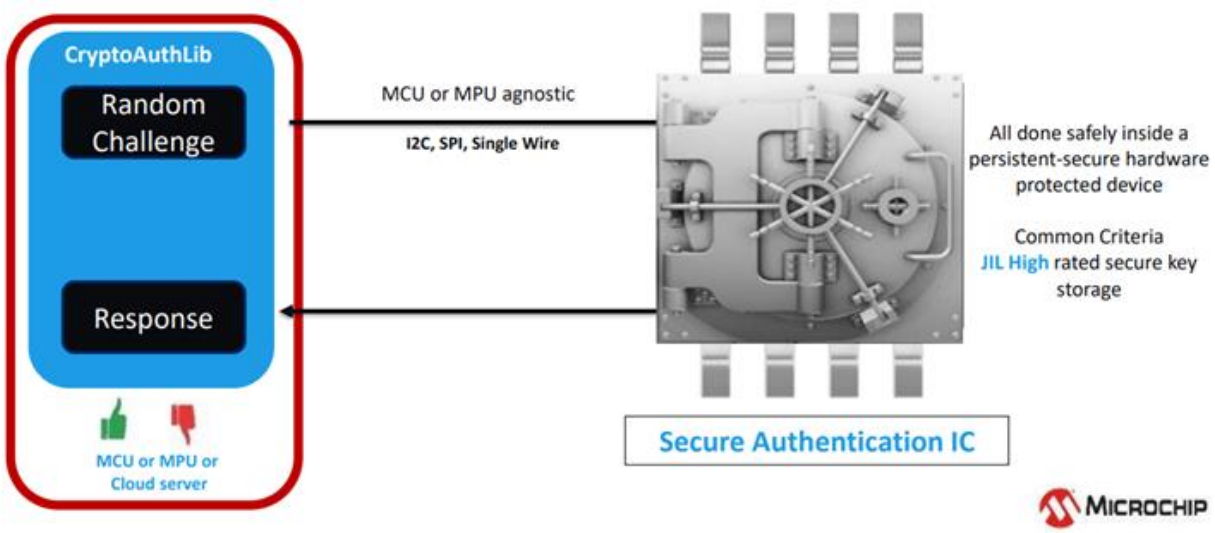

圖 1：安全身分驗證過程

主機 MCU 向即將託管機密資訊金鑰並擁有加密引擎的安全身分驗證 IC 發送隨機質詢。隨機質詢與金鑰一起饋入加密引擎中以產生回應。

不斷擴充的產品組合

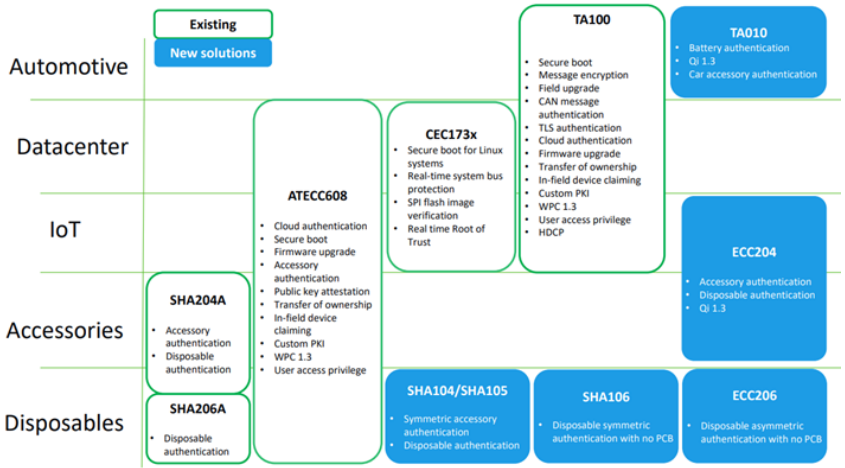

圖 2：Microchip 產品組合

我們的產品組合最近迎來了幾款新的解決方案。在汽車市場，我們推出了 **TA010**。對於配件和一次性用品，請查看我們新推出的 **ECC204** 以及 **SHA104**/**SHA105**、**SHA106** 和 **ECC206**。

這些新元件旨在提供最小可行性的加密加速器，同時保持較小的記憶體空間，進而優化成本。因此，上述元件僅支援 ECDSA 簽名和 HMAC/SHA256 等演算法。如需更完備的加速器，請查看 TA100 和 ATECC608 元件。

對稱身分驗證

對稱身分驗證是最簡單的一種身分驗證，主機只需要一個機密資訊金鑰就可以對用戶端（一次性用品/配件）進行身分驗證。

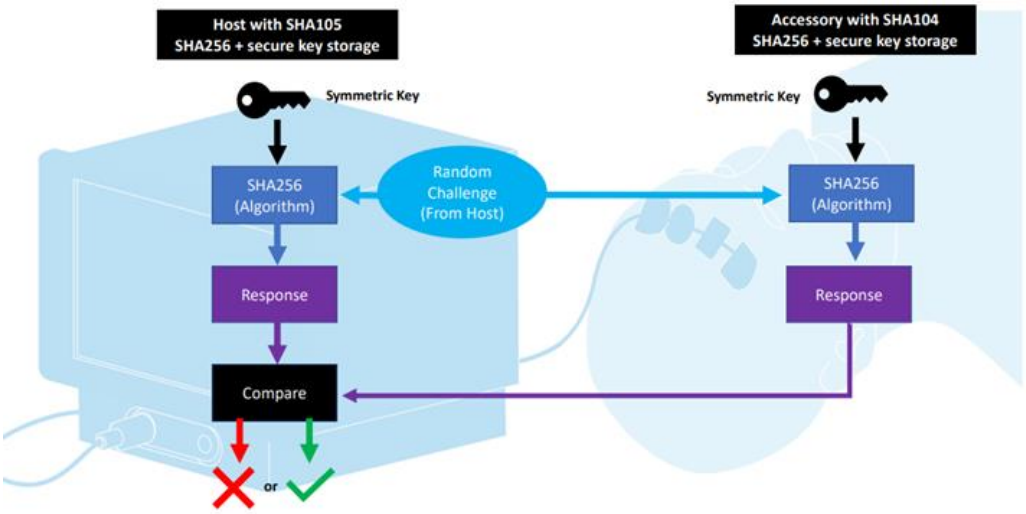

圖 3：對稱身分驗證的基本原理

我們將採用通俗易懂的方式進行解釋。以大腦感測器和主機為例。兩側都配有安全系統，左側為 SHA105 晶片，右側為 SHA104 晶片。主機向感測器發送質詢，以運行 SHA256 演算法來創建摘要或回應。兩側都使用對稱金鑰。配件/一次性用品所作出的回應隨後返回主機進行比較，確保兩個回應完全相同才能接收來自感測器的資訊。

此外，使用對稱金鑰多樣化可以更順暢實現這一目標。因為每個配件/一次性用品都有惟一的對稱金鑰，這有效降低了偽造每個金鑰和暴露整個系統的風險。

非對稱身分驗證

非對稱身分驗證（也稱為公開金鑰加密）使用兩種類型的金鑰（公開金鑰/私密金鑰）進行身分驗證。

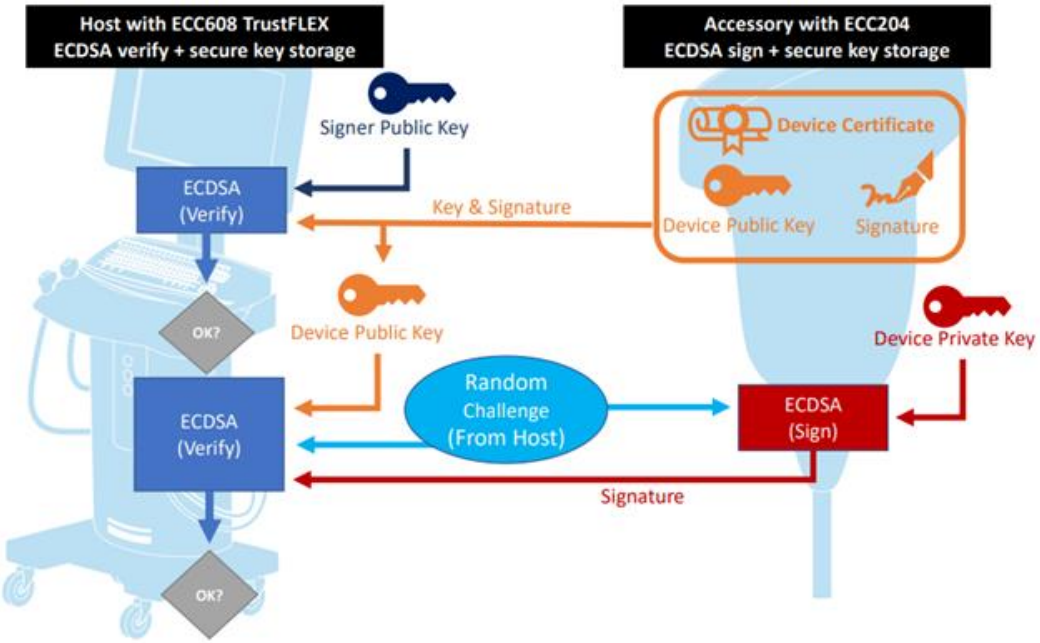

圖 4：非對稱身分驗證

在這種情況下，我們可以假設客戶與設備之間已經建立了認證（例如，類似於 Qi 1.3 標準認證），然後現在我們來看一下在嵌入式系統中，質詢回應是如何發生的。主機中有簽名人公開金鑰，配件中有設備公開金鑰和簽名。簽名是透過私密金鑰對隨機質詢執行的 ECDSA 簽名操作的輸出。設備公開金鑰透過簽名人公開金鑰進行驗證，設備公開金鑰本身用於驗證簽名。之後，系統可以繼續執行其操作並接受進一步的資訊。

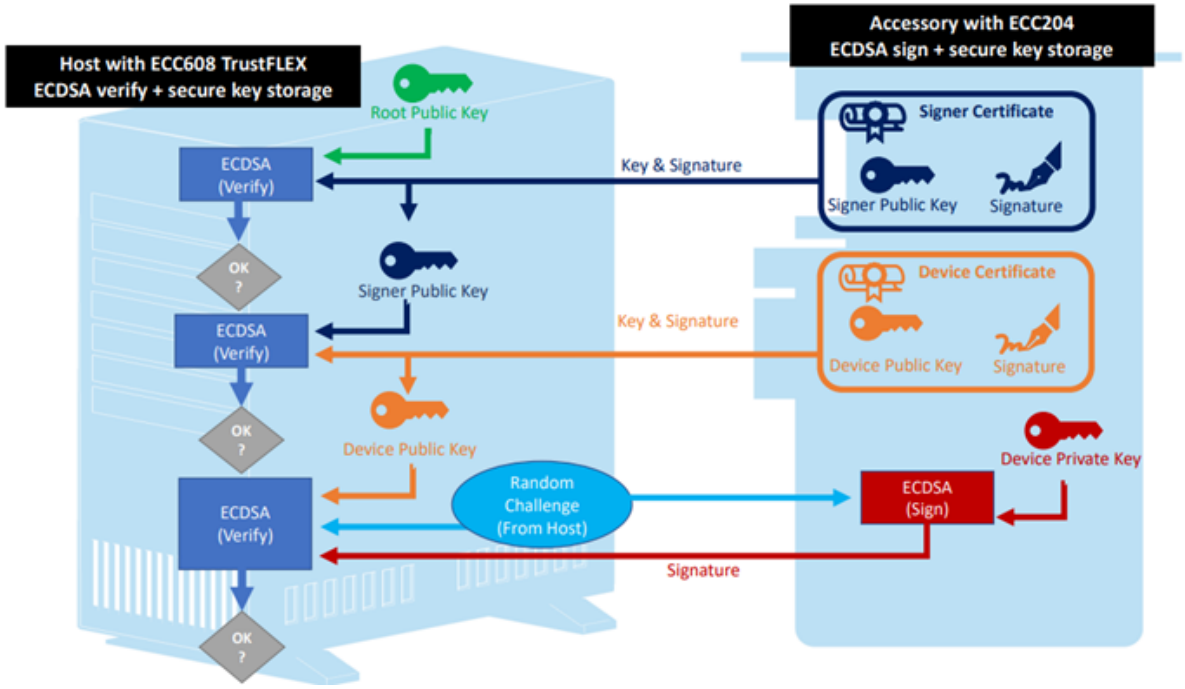

圖 5：使用根公開金鑰的非對稱身分驗證

這種情況稍微複雜一些，因為我們現在添加了一個根公開金鑰或 OEM 公開金鑰。我們需要驗證每個階段的公開金鑰，從簽名人公開金鑰（透過根公開金鑰驗證）到設備公開金鑰（透過簽名人公開金鑰驗證），並且需要驗證簽名是否合法。一旦系統確認簽名正確，即可進入下一步。

寄生電源：從 3 接腳縮減為 2 接腳

當封裝中的接腳數受限時，寄生電源至關重要。我們在元件前面添加了一個整合電容，它能夠儲存足夠的電能來運行身分驗證計算並提供相關的回應。該電容使得從 3 接腳縮減為 2 接腳成為可能。一個接腳用作資料和電源接腳，即用於通信和供電；另一個接腳用作接地接腳。接腳數量得到縮減後，便無需在一次性用品中使用 PCB，進而降低系統級成本並簡化建置過程。

安全金鑰配置服務

Microchip 工廠配有硬體安全模組（HSM），我們客戶的設備都是在此進行加密操作。我們可以大量承接不同客戶的專案，並為其配置金鑰以及其他需要保密的資料。可信平臺將為您提供可用選項的概覽。

可信平臺設計套件

我們的 **DM320118** 是幫助您入門的基礎工具包，因為它可以與**可信平臺設計套件（TPDS）**和其他軟體工具搭配使用。務必要選用適合您的附加板。另外，我們還提供插座附加板。使用 TPDS 可以存取有關對稱/非對稱身分驗證以及 Qi 1.3 的範例教程。此外，TPDS 還提供 C 程式範例，精選安全身分驗證 IC 的配置器，以及在 Microchip 安全配置服務中完成引導流程所需的公用程式。

結語

我們的產品組合始終致力於讓您更輕鬆地進行安全身分驗證，使用簡單的工具集進行快速開發，以及利用電子商務商店簡化流程。我們的產品適合大眾市場，支援低 MoQ，包括與 **CryptoAuthLib** 無關的配置和架構。

如需瞭解更多資訊，請訪問我們的**安全身分驗證網頁**。