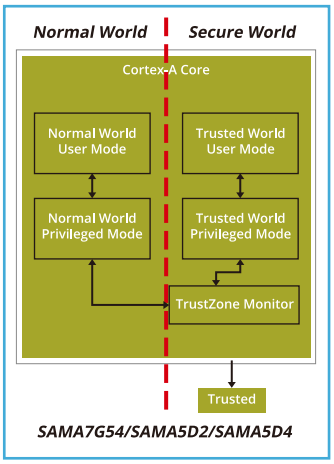
全面防護的信任區——探索ARM® TrustZone®

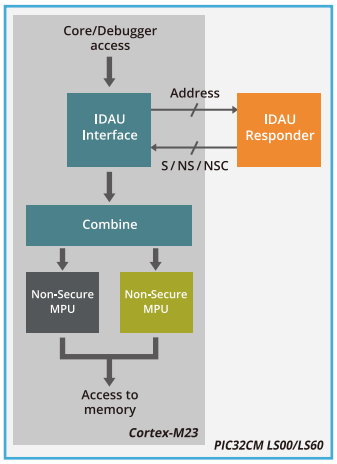
作者：張裕坪　應用工程師

SMART | CONNECTED | SECURE

小百科

ARM® TrustZone® —— 硬體的安全解決方案，提供了一個基於硬體的安全執行環境。您可以在整合 TrustZone 的微處理器 (MPU) 或微控制器 (MCU) 平台上，建立普通世界 (Normal World) 和安全世界 (Secure World) 兩個虛擬並且完全隔離的執行環境。TrustZone 的安全世界 (Secure World) 是一個受保護的執行環境，可以執行 TrustZone 監控器 (TrustZone Monitor)，或使用 IDAU (Implementation Defined Attribution Unit) 執行安全管理 (Security Management)，管理在安全世界受保護的應用程式和資料，以及防止駭客或惡意軟體，嘗試從普通世界的操作系統中，非法操控系統或竊取敏感的機密資料。





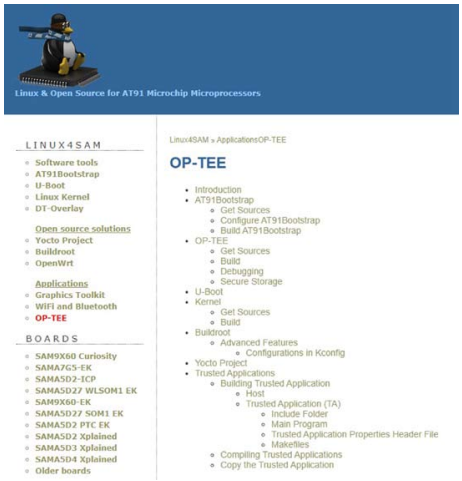
TrustZone 除了提供安全執行 (Secure Execution) 環境外，也提供了下列的安全功能：

- **安全啟動 (Secure/Trusted boot)：**在啟動過程中，驗證系統的啟動程序，確認系統啟動過程中沒有被攻擊或修改。
- **安全儲存 (Secure Storage)：**提供一個安全的存儲區域，儲存敏感資料、金鑰和證書等，防止被駭客或惡意軟體竊取。
- **安全通訊 (Secure Communication)：**交換敏感資料和命令時，提供一個安全的通訊通道，防止中間人攻擊和竊聽。
- **安全除錯 (Secure Debugging)：**在除錯受保護的應用程式和操作系統時，提供一個安全的除錯環境，防止除錯信息被竊取。

Microchip SAMA7G54 (ARM Cortex®-A7)、SAMA5D2 (ARM Cortex-A5) 和 SAMA5D4 (ARM Cortex-A5) 系列微處理器 (MPU) 和 PIC32CM LS60 (ARM Cortex-M23) 微控制器 (MCU) 都整合了 TrustZone，並且被廣泛應用於數據集中器、支付終端機、物聯網裝置、智慧型穿戴裝置、可攜式醫療設備... 等應用，保護阻斷遠端或物理攻擊。

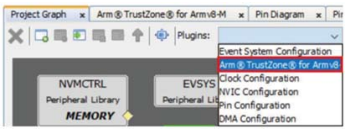
在軟體方面，Microchip 提供 OP-TEE (Trusted Execution Environment) 在 SAMA7G54、SAMA5D2 或 SAMA5D4 系列微處理器 (MPU) 的 Linux 平台啟用 TrustZone。

OP-TEE



Microchip 圖形用戶界面 (GUI) 的 MPLAB® Code Configurator (MCC) TrustZone Manager 簡化了配置 PIC32CM LS60 微控制器 (MCU) 的 TrustZone。使用 Microchip 可信平臺設計套件 (TPDS，Trust Platform Design Suite) 工具，可安全地配置金鑰和證書。

The Arm® TrustZone® for Armv8-M manager (MCC)



Trust Platform Design Suite Tools (TPDS)

如您想進一步了解 Microchip 整合了 TrustZone 的微處理器和微控制器，請參考以下官方網站或掃描 QR code。亦歡迎與我們經驗豐富的設計團隊聯繫。

https://www.microchip.com/en-us/products/microcontrollers-and-microprocessors/32-bit-mpus/sama7

https://www.microchip.com/en-us/products/microcontrollers-and-microprocessors/32-bit-mpus/sama5/sama5d2-series

https://www.microchip.com/en-us/products/microcontrollers-and-microprocessors/32-bit-mcus/pic32-32-bit-mcus/pic32cmlx

https://www.linux4sam.org/bin/view/Linux4SAM/ApplicationsOP-TEE

SAMA7G54　SAMA5D2　PIC32CMLS60　OP-TEE

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

MICROCHIP

SMART | CONNECTED | SECURE