psacertified™

arm

PUFsecurity

PSA-Certified 認證的加密協處理器 -- 為 Arm 生態系統提供完整的安全防護

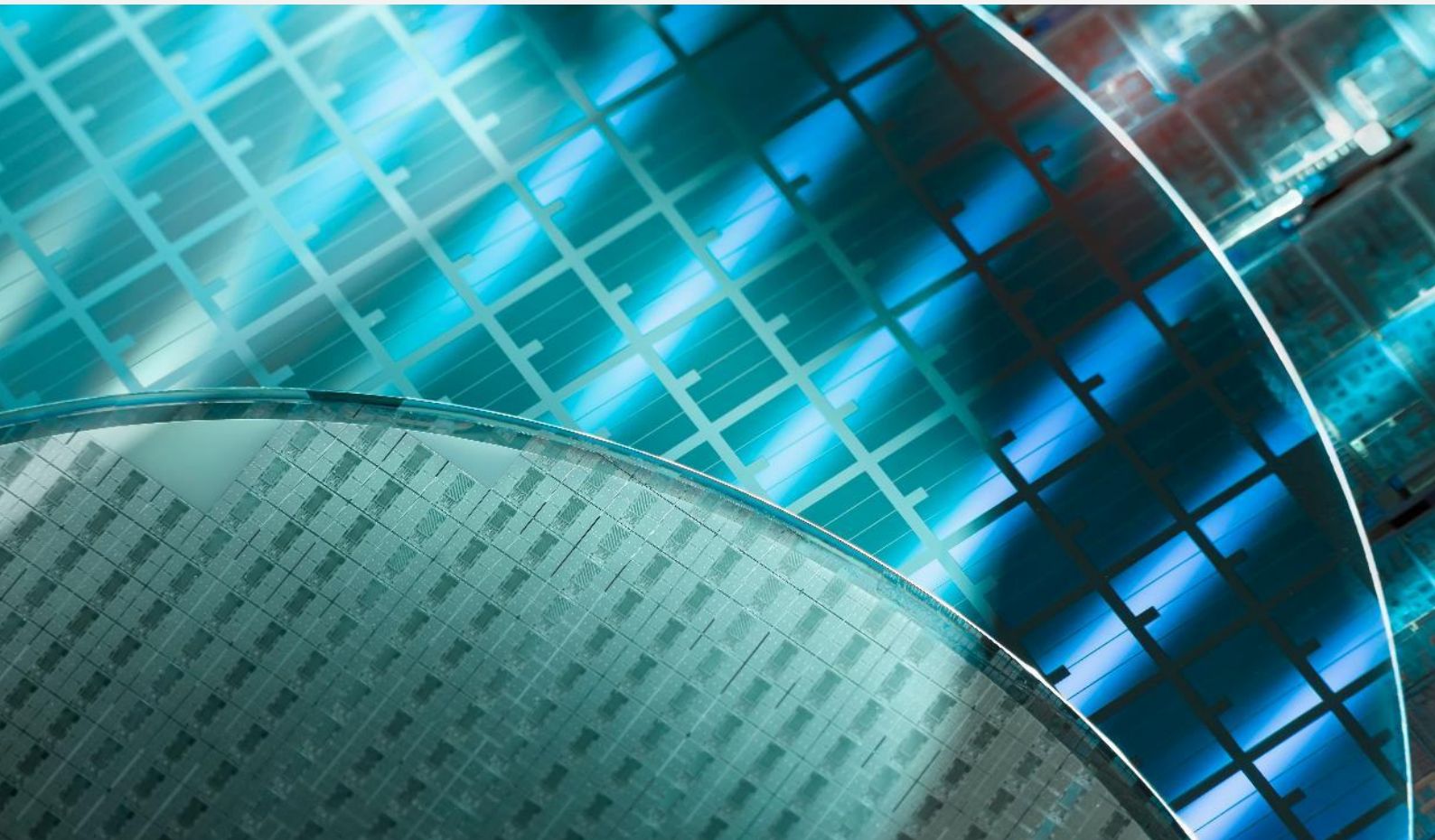
Whitepaper

Lawrence Liu (劉持志)

Dr. Evans Yang (楊青松)

Stephanie Smith

March 2023



晶片到系統的安全性

在過去的五年裡，Arm 通過安全宣言重申了保護其架構安全的承諾。它為半導體行業做了明確的宣示。在面對當今計算所面臨的日益嚴峻的威脅時，單依靠軟體防護只能在一定程度上緩解漏洞，因此，需要硬體解決方案為設備奠定堅實的基礎，支持整體系統安全運行。

現實情況是，電子設備需要一個全面的安全生態系統來提供協作和分層的解決方案。從物聯網、人工智能，到移動設備，幾乎沒有一個計算過程不涉及 Arm 架構。他們也因此號召合作夥伴一起推動 “強化晶片到系統的安全性” ，並為硬體級別提供全面的保護。

Standardizing IoT Security with PSA Certified
PSA Certified 建立物聯網安全標準

由於物聯網的成長太過快速，使得該相應落實的安全性標準訂定工作相對落後，這促使 Arm 在 2019 年與合作夥伴率先提出了 PSA Certified 認證標準。他們的目標是提倡將物聯網安全主動納入晶片設計考慮，以保護物聯網設備免受侵害及惡意攻擊。憑藉一套強大的通用標準，PSA Certified，有助於改善各種物聯網設備、應用程式和解決方案提供商之間安全協議的碎片化。

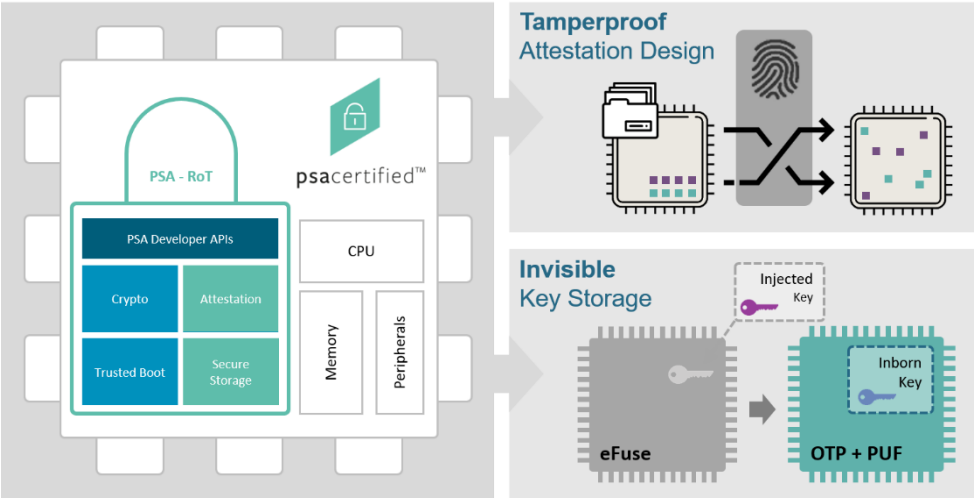


圖 1：PSA Certified 對物聯網信任根的標準要求

PSA Certified 通過與第三方實驗室合作，來檢驗設計的安全性，並推廣可廣泛通用的基礎安全功能。此舉不僅是為了減輕終端設備使用者對隱私侵犯的擔憂，更是為了解決供應商近在眼前的挑戰--各國政府即將推出的物聯網安全要求。由於存在各種類型的物聯網產品，因此 PSA 認證計劃也提供不同級別的認證。其中包括 PSA Certified Level 1、PSA Certified Level 2、PSA Certified Level 2 Ready 和 PSA Certified Level 3。這樣的安全級別分級反映了“物聯網安全沒有一刀切的解決方案”的現實。

PSA Certified Level 1 提供廠商以調查問卷的方式完成第三方實驗室的審核，但未進行實驗室內的實際測試。廠商並應證明該送審的物聯網晶片/設備/軟體設計遵循了物聯網威脅模型、PSA Certified 的 10 個安全目標以及全球政府指南要求的最佳安全實踐。

PSA Certified Level 2 和 PSA Certified Level 3 認證旨在衡量安全穩健性，故需要在實驗室中進行測試。測試內容包括使用選定的一系列純軟體攻擊，PSA Certified Level 3 則還需通過物理滲透評估（包括旁通道分析）。基於對硬體安全的關注，PSA Certified Level 2 和 PSA Certified Level 3 認證要求評估目標（TOE）必須有信任根（RoT）並滿足九項安全功能要求才能獲得認證。這些功能包括：

1. Initialization 安全啟動
2. Software Isolation 軟體隔離
3. Secure Storage 安全存儲
4. Firmware Update 韌體更新
5. Secure State 安全狀態
6. Cryptography 算法
7. Attestation 驗證
8. Audit / Debug 審核/除錯
9. Physical 物理防護

注意到這九個功能與 1 級認證中八個要求之間的重疊，因為安全硬體信任根 (HRoT) 自然必須遵循最佳安全實踐。

PSA Certified Level 2 Ready 可以被視為幫助公司獲得 PSA Certified Level 2 和 PSA Certified Level 3 的基石。隨著科技的演進，現代化晶片設計變得越來越複雜，當今產品設計可能會包含來自第三方專家的一個或多個 IP。這導致所需的人力資源和預算緊張，整體產品開發時間也縮短了。採用通過

PSA Certified Level 2 Ready 的 IP 對產品提供了安全的保障，且有助於縮短最終產品設計通過安全認證所需的時間。

獲得 PSA Certified Level 2 Ready 認證的加密協處理器

熵碼科技的 PUFcc 加密協處理器就是通過 PSA Certified Level 2 Ready 的例子。

PUFcc 將硬體信任根(PUF、Secure OTP 、TRNG)與全套加密加速器相結合，形成一個兼容性極強的安全 IP 模塊，可輕鬆集成到各種系統架構中。這種 “現成的” 解決方案使設計人員能夠 “即插即用” ，輕鬆實現系統所需的安全協議。

PUFcc 可以安全地執行高機敏的工作，這些機要操作在執行上與非機敏功能（通常由主系統負責）以硬體隔離的方式分開，改在以防篡改設計保護的安全邊界內執行。此外，PUFcc 是一個通用的集成安全 IP 模塊，支持所有常見的密碼算法，允許使用者構建各種安全協議。

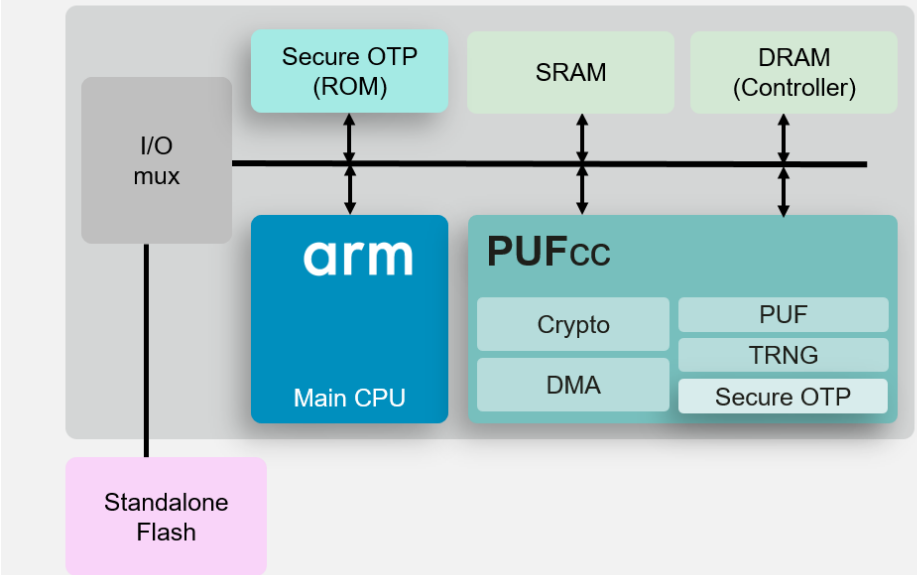


圖 2：PUFcc 的典型集成圖

PUFcc 作為加密協處理器並在安全邊界內執行各項的操作，其設計必須能讓系統無條件地信任。 PUFcc 的任務是保障整體系統安全性，特別是當無法確保 PUFcc 安全邊界之外的組件，例如系統內存、總線和共享系統總線的其他設備等，是100%安全的情況下。上述這些組件都是黑客為了獲得系統訪問或控制權、常見的攻擊目標。

熵碼科技已為 PUFcc 完成 PSA Certified Level 2 Ready 的認證，確保 PUFcc 能夠滿足可信任和隔離子系統的安全要求。具體地說，PUFcc 通過了安全啟動、安全存儲、韌體更新、安全狀態和加密算法的測試，是矽智財所能通過的所有項目。

加密協處理器中的信任根功能

安全啟動意味著評估目標需要確保只有授權的軟體才能在設備上執行。PUFcc 通過使用可信韌體 M (TF-M) 包中的 MCUboot 引導加載程式(boot loader)，在安全啟動(secure boot)流程中驗證經簽署的啟動代碼(boot code)來實現此目的。值得關注的是，PUFcc 是通過內部生成了用於此安全啟動的硬體密鑰而節省了外部生成密鑰與註入的各項成本。

安全存儲可防止私人數據被複製或從設備中竊取。 PUFcc 通過基於關聯數據認證加密（AEAD）安全數據策略的 AES（GCM 模式）實現安全存儲，保護私有系統數據的完整性和真實性。用於此安全數據策略的密鑰源自硬體唯一密鑰 (HUK)，只有 PUFcc 才能訪問該密鑰，該密鑰源自晶片內置的物理不可複製功能 (PUF)。透過 PUF 能確保每個 PUFcc 的 HUK 都是唯一且完全隨機的。

韌體更新（或安全更新），與安全啟動有間接關聯，是設備允許進行的唯一授權更新。然而，更新後的韌體的執行仍由安全啟動（初始化）流程完成。 PUFcc 通過限制對韌體映像槽的寫入權限來實現此目標，在安全更新過程中只允許寫入經正確簽名的韌體映像。然後，在安全啟動過程中，以最新的韌體映像檔執行啟動，同時更新安全計數器至與韌體的最新版本相匹配來防止任何對韌體映像進行回復的動作。

安全狀態將可信服務、低信任服務和不可信服務相互隔離。通過安全分區管理器（SPM），在 PSA 韌體框架的一部分中，如果分區之間的隔離出現任何錯誤，將通過 panic (interrupt) call 終止該進程。 PUFcc 以此建構了一個安全邊界，將安全/非安全操作之間安全地隔離。

加密功能支持著關鍵的系統安全功能，例如安全生命週期、隔離、安全存儲、安全驗證、安全啟動以及數據的安全加載和綁定。 PUFcc 支持全套加密算法，例如對稱/非對稱密碼、HASH、MACs 和 AEAD，以滿足各式密碼安全功能要求。

由於 PUFcc 作為 IP，並非設計為獨立產品，最多只能做到 PSA Certified Level 2 Ready 認證。要通過 PSA Certified Level 2 或 PSA Certified Level 3，取決於更大的集成系統來實施，以完整其他安全功能要求，包括軟體隔離、驗證、審核和除錯。

CoreLink SSE-200 Integration

PUFcc 的 PSA Certified Level 2 Ready 認證是使用 Arm MPS3 評估板進行的。 Arm CoreLink SSE-200 子系統的 FPGA 實現（如應用筆記 AN524 中所述）與 PUFcc 以及 MPS3 板上的可信韌體-M 端口集成。 CoreLink SSE-200 是適合用作 IoT SoC 基礎的預組裝組件（包括兩個 Cortex-M33 內核）的集成，源自 Arm 系統 SIE-200 庫。 Cortex-M33 內核的低功耗使得基於 CoreLink SSE-200 的系統成為邊緣物聯網應用的理想選擇。

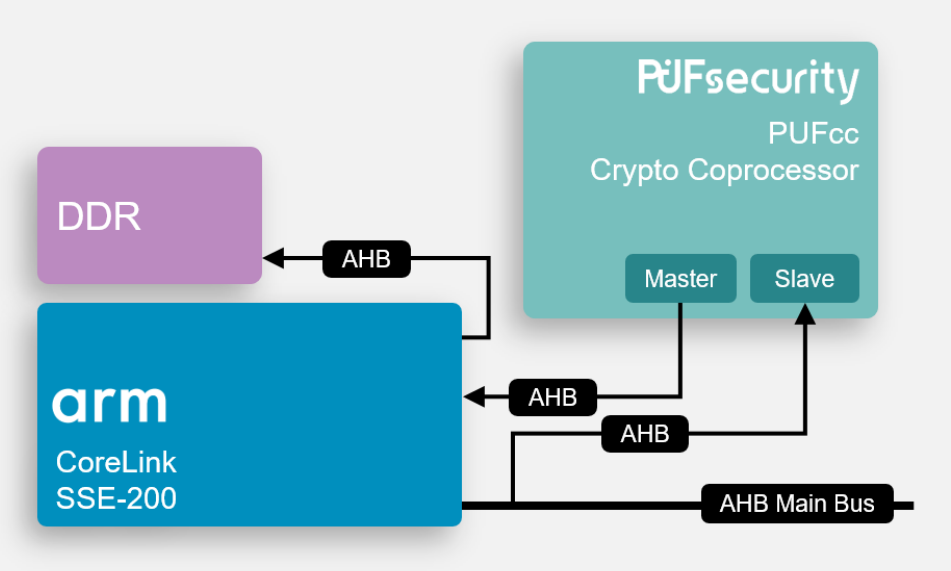


圖 3：Arm SSE-200 子系統上的 PUFcc 集成

PUFcc 旨在提供構建 PSA-RoT 的原始元素，將唯一標識符 (PUF)、安全存儲 (OTP)、TRNG 和加密引擎組合進一個支持加密操作的安全 IP 中。因此，PUFcc 可以用作安全處理環境 (SPE) 內的外圍設備。由於加密密鑰可以由信任根 (PUFcc) 本身在內部生成，因此避免了密鑰洩漏的風險，從而可以將 PUFcc 視為在其自己的安全邊界內。

為了與 CoreLink SSE-200 子系統集成，PUFcc 使用 AHB 和 APB 總線進行連接。 PUFcc 的 AHB 主機鏈接到 CoreLink SSE-200 安全管理控制器 (MSC)，以便根據 PUFcc 操作的需要向屬性設置單元 (IDAU) 發送請求，例如通過 PUFcc 的直接內存訪問模塊 (DMA)訪問的外部存儲器。 APB 從屬總線模塊連接到 CoreLink 的外設保護控制器 (PPC)，以接收來自 CoreLink SSE-200 的安全和非安全請求，作為 “Expansion 1” 接口的一部分。

Corstone SSE-300 Integration

除了 CoreLink SSE-200 之外，此認證過程還使用具 Trusted Firmware-M 端口的同類型評估板 Arm MPS3 來演示 PUFcc 與 Corstone SSE-300 子系統的集成，如應用筆記 AN552（軟核單元模型 – SM）。 AN552 具有一個帶自定義數據路徑擴展的 Cortex-M55 和一個 Ethos-U55 機器學習處理器。

與 CoreLink SSE-200 一樣，Corstone SSE-300 是從 SIE-200 庫中選擇的預組裝元素的集合（在本例中添加了 SIE-300 庫）。憑藉更強大的 Cortex-M55 內核，基於 Corstone SSE-300 的系統非常適合需要高性能的應用，如 AIoT。

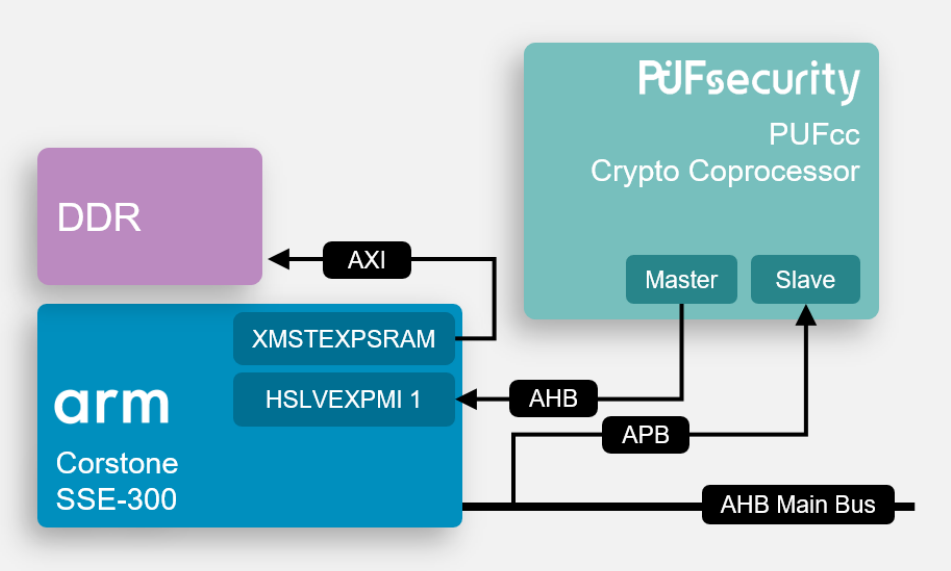


图 4：Arm Corstone SSE-300 子系统上的 PUFcc 集成

PUFcc 與 Corstone SSE-300 子系統的集成與 SSE-200 的情況非常相似，後者也使用 AHB 和 APB 總線。 PUFcc 的 AHB 主控再次連接到 CoreLink SSE-300 中位於從屬主擴展接口 (HSLVEXPMI1)的安全管理控制器 (MSC)。最後，APB 從屬總線模塊再次連接到 AN552 內存映射的非安全和安全外圍區域中的 Corstone APB 外圍保護控制器 (PPC)。

總結

Arm 的物聯網整體解決方案是一項目光遠大的計劃，旨在推動物聯網行業下一階段的發展。 PUFcc 是眾多 PUFsecurity 解決方案中第一個獲得 PSA 認證計劃認證的解決方案。因此 PUFsecurity 計劃作為合作夥伴與 Arm 攜手合作，促進安全的物聯網世界並保護我們互聯的世界。