Compliance Brief

THALES

CYBERSECURITY

強化 Caliptra 安全晶片設計合規指引

cpl.thalesgroup.com

THALES

CYBERSECURITY

Caliptra 是一個專爲資料中心系統單晶片（SoC）平台所設計的開源信任根（RoT）架構，提供可直接整合至任何現代資料中心級晶片（CPU、GPU、TPU、DPU 或 smart SSD）的統一開源建構模組。

Caliptra 的內部組成為何？

Caliptra 提供實際可用的程式碼，包含以下元件：

1. 硬體 RTL（矽邏輯）：實體電路區塊的設計藍圖，以開源的 RISC-V 處理器核心為基礎建構。
2. 密碼學加速器：專用硬體，可快速處理資安演算法，而不會拖累主要 CPU 的效能。最新更新（Caliptra 2.1）甚至納入了後量子密碼學（如 ML-DSA 與 ML-KEM），以防範未來量子電腦的攻擊。
3. 韌體：運行資安區塊所需的不可竄改 ROM 及執行期韌體。

透過使此架構公開透明且開源，Caliptra 成為伺服器或加速器晶片的「資安錨點」，提供可供上層資安服務建構的可信任基礎。

什麼是 Caliptra？

Caliptra 是一個提供標準化**晶片信任根**（Silicon Root of Trust，RoT）的開源硬體資安專案。該專案於 2022 年由 AMD、Google、Microsoft 及 NVIDIA 等業界巨頭共同創立，目前由 CHIPS Alliance 與開放運算專案（Open Compute Project，OCP）共同管理。

Thales 如何與 Caliptra 規範接軌

Thales 的 HSM 解決方案能協助企業組織與 Caliptra 的密碼基礎架構規範保持一致。

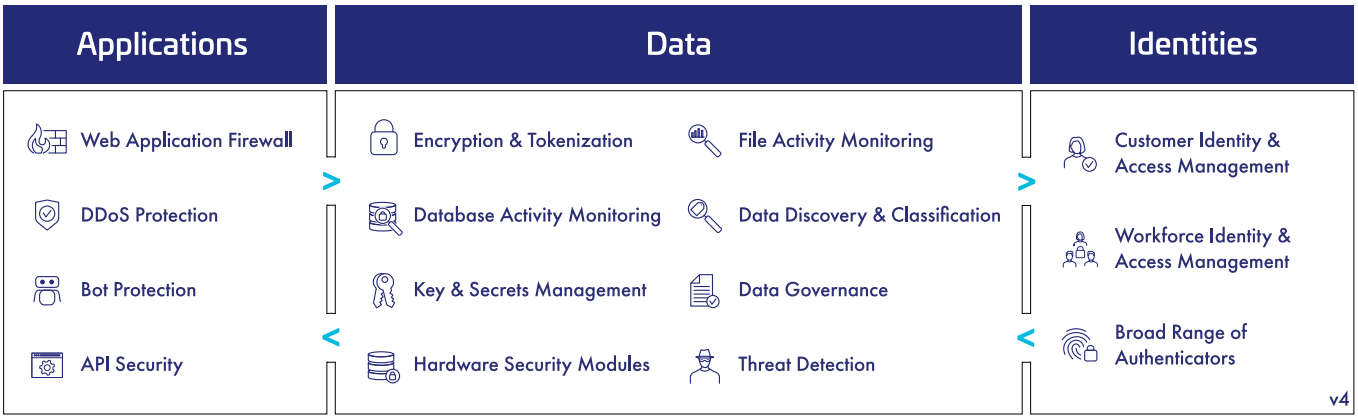
需求	Thales 的協助方式
Caliptra：資料中心系統單晶片（SoC）信任根（RoT）	
合規與認證需求 • 當雲端供應商希望針對 PCIe 連結傳輸中的加密進行 **FIPS 認證（FIPS 140-3 L3）**，且該加密根源自 Caliptra 執行個體所產生的 ASIC 身份時，即與本項相關。	• **密碼模組認證** 提供通過 FIPS 140-3 Level 3 驗證的 HSM，作爲製造 PKI、憑證簽發、簽章作業及生命週期金鑰管理的信任錨點，支援符合 FIPS 規範的生態系。
已知答案測試（KAT）支援 • 爲取得密碼模組認證，系統開機時必須執行預先運作自我測試，**實作 KAT** 是取得 **FIPS 認證**的必要條件。	• **認證所需的強制密碼自我測試** 提供經獨立驗證的密碼服務與自我測試機制，與支援 PKI 基礎架構的 FIPS 運作需求保持一致。
NIST 合規需求	
• UDS 種子與場熵必須使用加密安全的隨機數產生器（**CSRNG**）進行統計唯一性產生，並需符合 **NIST 熵源認證 SP 800-90B** 標準的熵源提供種子。 • Caliptra Checklist and Evaluation Methodology	• **裝置身份與金鑰的安全產生** 提供經驗證的熵值產生能力，用於產生及保護製造金鑰、CA 金鑰及配置機密。 • **唯一裝置身份根機密** 在製造／配置期間產生、包裝、注入或保護裝置身份素材及相關的憑證簽發工作流程。

需求	Thales 的協助方式
• **IDevID 憑證**（包含 CA 憑證）必須遵循指定格式與加密標準（例如金鑰大小和演算法必須符合 NIST 指南）。 • Caliptra Checklist and Evaluation Methodology	• **裝置身份與認證** 產生並保護用於簽發符合 NIST 密碼要求之 IDevID 憑證的根 CA 與中間 CA 金鑰。 • **信任建立** 保護 CA 私密金鑰，並支援 Caliptra 裝置身份生態系的憑證生命週期作業。
後量子密碼學（PQC）	
• Caliptra 2.x 以 **PQC 合規**爲目標。 ◦ Caliptra Trademark Audit Process • Caliptra 透過 Adams Bridge 納入了 **ML-DSA（FIPS 204）** PQC 實作 ◦ Adams Bridge Hardware Specification - 後量子密碼學 IP 核心（ML-DSA，FIPS 204）。 ◦ Adams Bridge README	• **朝向未來的抗量子資安** 支援 NIST 核准的 ML-KEM（FIPS 203）與 ML-DSA（FIPS 204），與 Caliptra 規劃中的 PQC 演進方向一致，並支援未來啟用 PQC 的配置及憑證工作流程。 • **PQC 簽章與認證** 作爲 PQC 證書頒發機構和簽名基礎設施的安全後端平台，同時 Caliptra 將 PQC 功能整合到設備端。
Caliptra 1.x：需要 LMS 與 ECDSA。 • Caliptra 提供要求在 **ECDSA 簽章**之外另附 **LMS 簽章**的選項。 • 建議從地理分散的**多台 HSM** 建立 LMS 樹。	• **簽章金鑰的硬體保護：** 提供通過 FIPS 140-3 Level 3 驗證的環境，用於保護韌體簽章及認證工作流程中使用的私密簽章金鑰。 • **後量子數位簽章：**支援 NIST 核准的 LMS/HSS、CNSA 2.0 標準-用於韌體簽章的 LMS 簽章金鑰，提供硬體支援的保護。 • **分散式信任基礎架構：** 支援地理分散式環境的部署，提供具韌性且高可用性的密碼服務，與 Caliptra 分散式 LMS 日誌結構合併樹建立的建議方向保持一致。 • NIST CAVP (PQC) 驗證 (#39968)
Caliptra 2.0：需要 MLDSA、ML-KEM、ECDSA、ECDH。 • Caliptra 從 **2.0** 版本起提供在 **ECDSA** 之外使用 **ML-DSA-87** 簽章的選項，以支援 FIPS 204 及類別 5 的 CNSA 2.0 需求。 • Caliptra 提供密碼服務以支援 **ML-KEM（除 ECDH 外）**金鑰交換。	• **後量子數位簽章：** 支援 ML-DSA（FIPS 204），爲憑證簽發、韌體簽章及認證所使用的後量子簽章金鑰提供硬體支援的保護。 • **後量子金鑰建立：** 支援 ML-KEM（FIPS 203），實現硬體保護的抗量子金鑰建立，用於安全配置和加密基礎設施。 • NIST CAVP (PQC) 驗證 (#39968)
通用密碼模組需求	
嚴格的**金鑰產生與保護**需求， • Caliptra Checklist - Asset Management - UDS 種子保護需求 • Caliptra Hardware Specification - Key Vault	• **密碼金鑰的安全儲存與使用** 爲製造、配置、認證及 PKI 金鑰提供硬體級的保護。Caliptra Key Vault 在配置完成後保護設備駐留金鑰。
實體**防竄改**與偵測機制， • Caliptra Hardware Specification - Physical security features 包含實體安全功能。	• **防範實體攻擊** 提供 FIPS 140-3 Level 3 實體保護。Caliptra 在裝置內部提供 SoC 層級的實體安全功能，兩者結合，可實現從後端信任錨點到終端設備的端對端防護。
密碼作業的完整性**保證**。 • Caliptra ROM Threat Model • Caliptra Security Assessment Report	• **防範韌體或加密竄改** 保護用於韌體簽章與認證基礎架構的簽章金鑰。Caliptra 在裝置信任根內部驗證韌體完整性。

需求	Thales 的協助方式
熵源**認證** • Caliptra Checklist - Entropy Requirements - 符合 NIST SP 800-90B（熵源驗證）與 NIST SP 800-90A（DRBG 機制）合規要求。 • Caliptra: A Datacenter System on a Chip (SoC) Root of Trust (RoT)	• **法規合規** 透過熵值產生及經驗證的密碼模組，支援後端信任基礎架構的合規需求。

Thales 在三大核心資安領域提供全方位的網路資安解決方案：應用程式安全、資料安全以及身份與存取管理。

Security for What Matters Most



應用程式安全： 在雲端、地端或混合模式下大規模保護應用程式與 API。我們市場領先的產品組合包含針對分散式阻斷服務攻擊（DDoS）及惡意機器人攻擊的網頁應用程式防火牆（WAF）防護、API 安全防護，以及安全的內容傳遞網路（CDN）。

資料安全： 探索並分類混合 IT 環境中的機敏資料，並透過加密、代碼化及金鑰管理，自動在靜態、傳輸中及使用中的任何位置加以保護。Thales 解決方案同時能識別、評估及優先排序潛在風險，進行精準的風險評估，並識別異常行為、監控活動以偵測潛在威脅及驗證合規狀態，協助企業組織優先配置資源。

身份與存取管理： 為客戶、員工及合作夥伴提供無縫、安全且可信任的應用程式與數位服務存取體驗。我們的解決方案透過細緻的存取政策與多因素驗證（MFA），依據角色與情境限制內外部使用者的存取權限，確保正確的使用者在正確的時間取得正確的資源存取權。

企業組織可善用 Thales 在單一統一平台上提供的身份、應用程式及資料安全解決方案套件，立即達到合規要求，並持續維持合規狀態。立即聯絡我們！

關於 Thales

當今的企業與政府依賴雲端、資料和軟體來提供值得信賴的數位服務。因此，全球最知名的品牌與組織仰賴 Thales 協助保護機敏資訊和軟體，無論是在雲端、資料中心、裝置或網路上，不管資訊在何處建立、儲存或存取，皆能獲得保障。作為資料安全與軟體授權領域的全球領導者，我們的解決方案協助企業組織安全地遷移至雲端、自信地達成合規、從軟體中創造更多價值，並每天為數百萬消費者提供無縫的數位體驗。