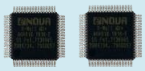
Enova 安全晶片技術與架構

– 經 FIPS140-2 2 級和 3 級驗證的單晶片密碼模組

ENOVA 西元 2000 年發明全碟加密 (Full Disk Encryption) 技術。	■ **ENOVA 發明的全碟加密技術全球獲得超過 16 個發明專利包括美國、中國、台灣、日本、韓國及加拿大。** ■ **全碟加密技術以磁碟機介面速度(又稱為 ON-THE-FLY) 自動加密整個磁碟，從啟動磁區（磁區 0）開始，直至最大 LBA[1]。** ■ **磁碟機介面可以是 ATA/SATA、PCIe、USB 或其他。** ■ **通過 NIST CMVP 驗證的 AES XTS/CBC 256 位元[2]硬體即時引擎。**
為何需要全碟加密技術？	■ 保護磁碟機從啟動磁區到最大的 LBA 包括作業系統和應用程式的資料**機密性和完整性**[3]。 ■ 保護載具的磁碟機因**錯放、處理不當、被捕獲、丟失或被竊**時，仍可保護全部的敏感資料，因為透過私密金鑰與私密金鑰材料的加密擦除(Cryptographic Erase)，資料將保持加密狀態，避免被拆解分析。
什麼是 SED (自加密磁碟機) 和 TCG OPAL 磁碟機？	■ SED 是 FDE 技術的衍生，其即時加密機制透過磁碟機的內部控制器完成。 ■ TCG OPAL 硬碟在 FDE 技術層之上建構了一個 OPAL 軟體協定執行基於角色的身份驗證。 ■ SED 和 TCG OPAL 硬碟的私密金鑰均由內部控制器生成，這可能在私密金鑰的生成、儲存、傳播、銷毀和恢復過程中存在嚴重的安全漏洞。
 **FIPS 驗證是什麼以及它有多重要？**	■ **FIPS 140-2**[4] 透過 CAVP [5]和 CMVP [6]的嚴格流程**評估和驗證**目標加密模組經明確定義邊界的安全性實施，**並根據安全功能和保證等級逐步提高層級從 Level 1 到 Level 4**[7]。 ■ **ENOVA *X-Wall* MX+** 系列晶片獲得了 FIPS 140-2 Level 2[8]與 Level 3[9] (包括 FDE 及 TCG OPAL 功能)驗證，其具效能微調的 AES 256 位元引擎可高速加密靜止資料(Data-at-Rest)和傳輸中資料(Data-in-Transit)，包括雲端備份。
使用 ENOVA FIPS 驗證單晶片的額外好處	■ 低 SWaP（尺寸 7x7 毫米、重量和功耗）、具高性價比，易於部署[10]。 ■ **可保護所有的 SATA 標準磁碟。** ■ 作為**硬體信任根**，內建 CMVP 驗證的**真亂數產生器**，受 **Level 3 的物理安全邊界保護。** ■ **預動身份驗證**與 **ENOVA SafeBoot**，監控並保護啟動流程與應用軟體程式的真實性。
聯絡方式	www.enovatech.com | P: +886 3 577 2767 |電子郵件：contact@enovatech.net

注解:

1. **邏輯區塊定址(LBA)** 是磁碟機的一種磁區定址模式，其區塊長度為 **512 位元組**或 **4,096 位元組**。
2. **AES 256 位元加密**具有抗量子攻擊能力。在 2000 年時，主流的加密演算法仍是 **DES** 和 **TDES**。
3. **機密性**和**完整性**是現代 CIA 安全目標（機密性、完整性、可用性）的關鍵角色。
4. **FIPS 140-2（聯邦資訊處理標準）**將自 2024 年起遷移至 **FIPS 140-3**。
5. **CAVP（密碼演算法驗證計畫）** 評估並驗證所有 NIST 發布的加密演算法，是進入 **CMVP 流程**並最終獲得 **FIPS 認證**的前置條件。有些演算法會選擇僅止於此階段。
6. **CMVP（密碼模組驗證計畫）**會在明確界定的密碼邊界下，評估並驗證目標密碼模組。成功完成 CMVP 流程後即可獲得最終的 **FIPS 認證**。
7. **軟體密碼模組**只能在 **Level 1** 進行驗證；**硬體模組**則可以在 **Level 2 及以上等級**進行驗證。
8. **FIPS Level 2** 著重於**基於角色的身份驗證、安全策略、系統與通訊保護，以及組態管理**。詳情參見：https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/3675。
9. **FIPS Level 3** 在 Level 2 的要求基礎上，增加了**基於身份的身份驗證**與**防篡改功能**。
10. **ENOVA 晶片**可在約 **0.6W 功耗**下，持續進行 **SATA Gen 3 的高速加密作業**。