Enigma™

安全備份與零信任架構

基於 Enova FIPS 140-2/3[1] 安全模組的抗量子離線與異地備份解決方案

使用 Enigma 安全備份架構的額外好處

- Enigma 不只是安全技術，更是品牌信任與責任的象徵。採用低 SWaP[8]（尺寸、重量與功耗）設計、可擴展信任根，能整合至國防、航太、工控與企業基礎設施，兼容現有備份系統。

為何需要 Enigma Pathway 安全備份技術？

Enigma Pathway（ENIGMA）透過 FIPS 驗證晶片模組與抗量子加密演算法（PQC[2]），在資料產生、儲存與傳輸的每一階段，確保資料機密性、完整性與可追溯性。即使主系統、雲端遭入侵，或傳輸過程受威脅，資料與備份仍維持加密狀態，且金鑰不離開 ENIGMA 模組，保障加密資料安全。

Enigma 零信任備份與授權控制架構

Pathway Framework – Data - Centric Zero Trust Architecture[3]：
以資料為核心建立信任鏈，備份與回復皆以「資料真實性與完整性」為判準。確保 Data - at - Rest / Data - in - Transit / Data - in - Use[4] 全階段實現資料真實性與完整性驗證。

Enigma 抗量子備份加密模組

採用 AES-256[5] 與 PQC XMSS / LMS[6] 實時加密引擎，符合 NIST SP800-208 與 NIST CMVP。
內建真亂數產生器（TRNG[7]）與金鑰生命週期控制，符合國際安全標準。並以抗量子級安全守護，讓資料備份具備未來抵禦力。

Enigma 優勢

Enigma 提供可整合至客戶資料處理節點的零信任備份 Library / SDK，協助於既有系統中自動化建立從備份、傳輸到復原的信任鏈。支援私有雲、公有雲、邊緣與離線儲存等多種環境，更可符合美國國家安全局 CNSA2.0 之軟韌體簽章驗章需求。Enigma 對應全球資料防護治理框架，從 NIST、ISO 到歐盟，皆以資料主權與零信任為核心；經 FIPS 驗證模組構成政策層信任基礎，確保資料在任意環境下皆維持可控、可驗證與合規狀態。

注解

1. FIPS 140-2 / 140-3：美國聯邦資訊處理標準，針對加密模組安全性進行驗證，分為 Level 1 至 Level 4 等級。
2. PQC（Post-Quantum Cryptography）：抗量子加密，能抵禦量子電腦對傳統加密演算法的攻擊。
3. Zero Trust Architecture：零信任架構，要求每次資料存取都需重新驗證身份與完整性。
4. Data-at-Rest / Data-in-Transit / Data-in-Use：分別指靜止、傳輸及使用中資料的三階段保護。
5. AES-256：對稱式加密演算法，在量子計算假設下保有足夠安全裕度。
6. XMSS / LMS：美國NIST 批准的抗量子簽章演算法，用於備份驗證與金鑰綁定。
7. TRNG（True Random Number Generator）：真亂數產生器，提供高熵隨機性，確保金鑰不可預測性。
8. SWaP（Size, Weight, and Power）：尺寸、重量與功耗，常用於國防與嵌入式系統效能指標。

聯絡我們 www.enovatech.com | P：+886-3-577-2767 | 電子郵件：contact@enovatech.net