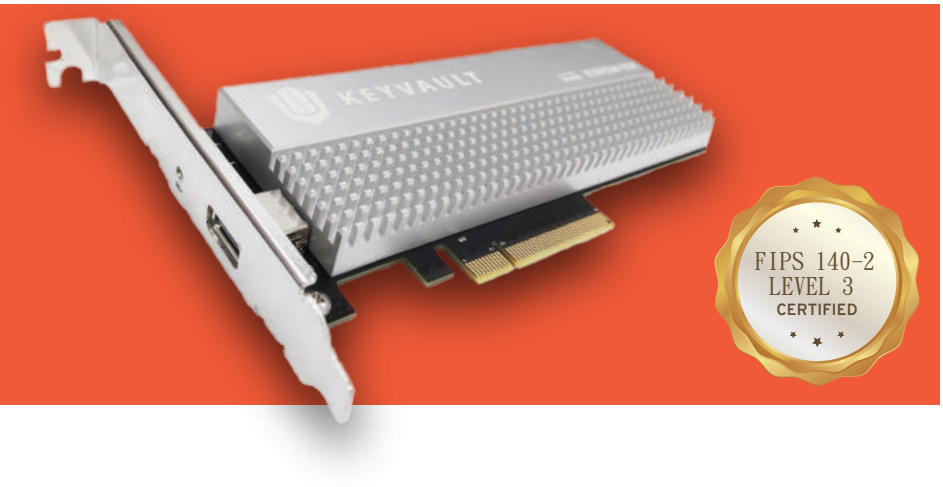
KEYVAULT



kvHSM

Hard security made easy

KeyVault™ PCIe HSM (kvHSM)，提供 「儲存金鑰」 與「執行密碼運算」所需的高安全硬體環境，是如金庫般強固的物理裝置。除了抵禦連網威脅、物理入侵及惡意篡改，其內嵌 CC EAL 5+ 認證的軍規級安全元件，更能抵禦多種硬體攻擊，如旁通道攻擊 (Side-channel Attack)。大幅提升金鑰安全，防止外洩。kvHSM 針對伺服器端的防護而打造，擁有 PCIe 高速介面，提供高速密碼服務，如數位簽章、雜湊函數、身分識別、金鑰完整生命週期管理等。

密碼貨幣交易所金鑰管理

密碼貨幣交易的核心，在於簽章時所使用的金鑰，金鑰如何管理，將左右交易的安全性。kvHSM 提供可高度客製化密碼演算法的平台，為使用者實現彈性應用，同時透過建全的金鑰管理機制，確保金鑰從生成、儲存、傳輸到銷毀的生命週期中，不洩漏任何機敏資料，保護使用者密碼貨幣資產。

身份認證伺服器 (物聯網生態系統) 及雲加密服務

物聯網雲 (IoT cloud) 除了提供服務給終端設備，還需儲存大量設備端資訊及行為，因此不管是動態傳輸或靜態儲存，物聯網雲皆曝露於竊聽和篡改的風險。駭客可能攔截消息，或在未經授權的狀態下入侵雲，因此通訊及身份認證前的數據加密，對於安全與業務連續性極為必要。 kvHSM 可嵌入雲端，作為雲端高速密碼引擎，用於數據保護、傳輸加密、認證伺服器、憑證簽署、韌體更新管理及金鑰生命週期管理 。

密碼演算法

- △Hashing: SHA-2, SHA-3, HMAC
- △RSA 2048
- △ECC with prime-field curves (up to 521 bits) and Edward curve
- △ECC Protocols: ECDSA, ECIES, ECDH, EdDSA (FIPS186-5)
- △AES 256 with modes: ECB, CBC, CFB, OFB, GCM, XTS
- △Random: AIS-31 (class PTG2) certi -fied TRNG with NIST SP800-90A Hash-DRBG
- △FPGA-based customizable crypto-engine for ECC and AES

運算效能

- △AES (256 bits XTS mode) data encryption/decryption up to ***1.6GB/s***
- △ECDSA (256 bits) up to ***10,000 tps***

認證與合規

- △FIPS 140-2 Level 3
- △CAVP: AES (ECB, CBC, CFB, OFB, GCM, XTS), ECDSA, HMAC, DRBG, SHA-2, SHA-3
- △CE/FCC

應用程式介面

- △PKCS#11
- △Native API

BYOK (Bring your own key)

雲服務導致使用者的金鑰與加密資料完全由雲服務供應商保管，使用者無從真正掌握金鑰位置與資料使用權限。然而無論是雲廠商或雲HSM提供商，都無法完全讓人信賴，這正是金融機構被規範金鑰落地的主要原因。kvHSM 的 BYOK 方案讓使用者在既有的雲服務框架下，將重要金鑰的管理和使用權拉回本地端。能完全掌握金鑰及機敏資料，大幅提升彈性與自由。 此外kvHSM 適用於市面上雲服務平台 ， 使用者導入時能有效節省建置及整合成本 。

實體安全

△SPA/DPA Countermeasures
△CC EAL 5+ Security Chip
△Tamper Response

核心應用功能

橢圓曲線密碼 (ECC) 數位簽章
硬體加解密卡能安全儲存數位簽章所需私鑰，並可支援標準與客製化曲線 。

雜湊函數 (SHA-2/SHA-3)
計算交易資訊之雜湊函數值，為區塊鏈中連接各區塊的核心算法。

分層確定錢包 (Hierarchical Deterministic Wallets, HD Wallet)
依據 BIP-32 生成任意數量私鑰並進行交易簽章。

先進加密標準 (Advanced Encryption Standard, AES) 資料加密
可用於磁碟、檔案或資料庫之內容加密。

客製化算法
可依據應用需求導入客製化密碼演算法，例如 MPC、Homomorphic encryption 與 PQC (Post-quantum Cryptography) 等。

對外介面

PCI Express (PCIe) ： 採用 PCIe Gen2 x 8 設計 ， 提供主機高速加密服務效能 。
USB ： 可使用分持 (Shamir Secret Sharing) 方式 ， 將金鑰透過硬體權杖進行備份與還原 。
狀態燈號 ： 顯示 kvHSM 目前狀態 ， 便於管理者維護 。

安全防護設計

實體安全防護 ： 為確保金鑰儲存與運作安全性 ， 若有外部入侵事件 ， 將立刻主動清除機敏資訊 。
防護外殼 ： kvHSM 外部覆蓋一防護外殼 ， 提供散熱與防窺探功能 。
AES 旁通道攻擊防禦 ： 抵擋 Hamming weight 模型的 DPA 攻擊 。

Wisecure Technologies 匯智安全

「匯智安全科技股份有限公司」，新一代「硬體安全模組」的品牌。秉持「匯聚智慧，透過硬體提供安全防護」的核心理念，聚焦於新經濟 (第四次工業革命) 時代數位防護的需要，以硬體安全模組保護既珍貴又脆弱的數位資產，協助使用者抵擋惡意攻擊，降低資料損毀所造成的威脅。