



kvHSM

Hard security made easy

核心應用功能



橢圓曲線密碼 (ECC) 數位簽章

kvHSM 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)

我們提供最新的雜湊函數，提供區塊鏈與簽章核心基礎。



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) 資料高速加密

kvHSM 最高能以 2.5GB/s 的優越效能，進行磁碟、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 (Multi-Party Computation)、Homomorphic encryption 與 PQC (Post-quantum Cryptography) 等。

KeyVault® 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，是如金庫般強固的硬體裝置。除了抵禦連網威脅、實體入侵及惡意篡改，其內嵌 CC EAL 5+ 認證的軍規級安全元件，更能抵擋多種硬體攻擊，如旁通道攻擊 (Side-channel Attack)。大幅提升金鑰安全，防止外洩。kvHSM 是針對伺服器端防護而打造，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，可滿足各種密碼貨幣算法需求，為使用者實現彈性應用，同時透過健全的金鑰管理機制，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

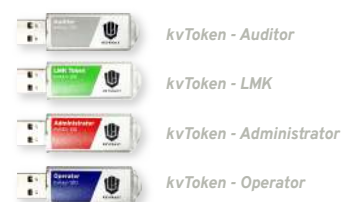
物聯網雲 (IoT cloud) 除了提供服務給終端設備，還需儲存大量設備端資訊及行為，因此不管是動態傳輸或靜態儲存，物聯網雲皆曝露於被竊聽和篡改的威脅。駭客可能攔截消息，或在未經授權的狀態下入侵雲，因此通訊及身份認證前的數據加密，對於安全與業務連續性極為必要。kvHSM 可作為雲端高速密碼引擎，用於數據保護、傳輸加密、認證伺服器、憑證簽署、韌體更新管理及金鑰生命週期管理。

BYOK (Bring Your Own Key)

雲服務中使用者的金鑰與加密資料完全由雲服務商保管，使用者無從真正掌握金鑰位置與資料使用權限。然而無論是雲服務商或雲端硬體安全模組提供商，都無法完全讓人信賴，這也是金融機構被規範不能將金鑰放在雲端的主要原因。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 提供市面雲服務平台之整合工具，使用者導入時能有效節省建置及整合成本。

硬體權杖管理機制

kvHSM 需搭配硬體權杖 kvToken (USB-based token) 進行管理。該機制讓使用者基於不同角色權限 (role-based) 持有權杖，如管理者 (administrator)、維運者 (operator)、稽核者 (auditor) 等，以權杖認證成功才能執行操作。該機制更將最重要的本地端主密鑰實體權杖化，以分持 (Samir Secret Sharing) 機制進行備份和還原，提升安全度，降低人為疏失可能性。



產品規格

實體安全	<ul style="list-style-type: none">· SPA/DPA Countermeasures· CC EAL 5+ Security Chip· Tamper Resistance
密碼演算法與功能	<ul style="list-style-type: none">· Hashing: SHA-2, SHA-3, HMAC· RSA 2048, 4096· ECC with prime-field curves (up to 521 bits) and Edward curve· ECC Protocols: ECDSA, ECIES, ECDH, EdDSA (FIPS186-5),ECMQV· AES 256 with modes: ECB, CBC, CFB, OFB, GCM, XTS· Random: AIS-31 (class PTG2) certified TRNG with NIST SP800-90A Hash-DRBG· Customizable crypto-engine· Accelerated ECC and AES crypto engine
加密與簽章效能	<ul style="list-style-type: none">· AES (256 bits CTR mode) data encryption/decryption up to 2.5GB/s· ECDSA (256 bits) up to 10,000 tps
API	<ul style="list-style-type: none">· PKCS#11· Native API
傳輸介面	<ul style="list-style-type: none">· PCIe Gen 2x8
安規認證	<ul style="list-style-type: none">· FIPS 140-2 Level 3 (in progress)· CAVP: AES (ECB, CBC, CFB, OFB, GCM, XTS), ECDSA, HMAC, DRBG, SHA-2, SHA-3· CE· FCC· RoHS

匯智安全科技股份有限公司是新一代「硬體安全模組」的品牌。秉持「透過硬體提供安全防護」的核心理念，聚焦於新經濟時代（第四次工業革命）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。