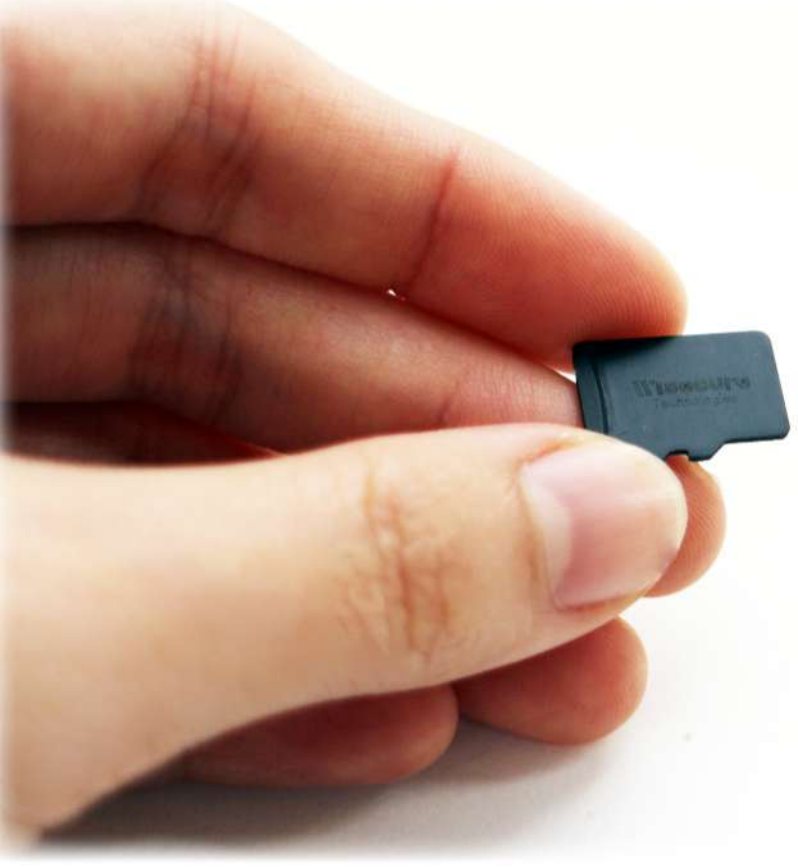
wisecuretech

VeloCrypt MicroSD HSM

SA Series

Features
Use cases
Security and cryptographic features
Hardware specification



High-speed Encryption
Optimizing Secure Communication

> 成為密碼系統關鍵的「密鑰」必須在最安全的環境中保管及執行密碼演算功能，通常會以 PCIe 卡等擴充卡形式的硬體安全模組管理和保護。然而 HSM 僅限於伺服器端使用，對於行動裝置與端點裝置的安全無法直接提供服務。

能解決此一問題的 VeloCrypt，擁有 HSM 的高度安全性與完整功能，同時具備 MicroSD 卡格式的優勢，可滿足行動裝置與端點裝置所需之密碼服務。其密碼功能包括加解密、密鑰生成及生命週期管理、數位簽章、認證等。極富巧思的設計使 VeloCrypt 的效能遠優於市面上其他同類型產品，能以 10MB/s 進行高速資料加密存儲。應用場景涵蓋安全認證、機密資料加密與存儲、安全通訊以及安全行動支付等。

產品特性

介面相容性
SDIO(secure digital input/output) 介面與簡單的服務存取模式，使 VeloCrypt 可以快速與使用者的各種裝置整合，無須修改裝置硬體，高度介面相容性讓客戶在導入安全防護時，得以加快產品開發生命週期。

實體安全
透過縝密的內部線路設計，以及嚴格的元件選用，確保密鑰在整個運作中能得到完全的保護，高規格安全元件針對當前盛行的旁通道攻擊也含防護。

系統安全
VeloCrypt 擁有嚴謹的韌體架構設計，以安全為優先，確保系統運作時機敏資料不外洩。

密碼服務與效能
VeloCrypt 提供高速對稱與非對稱演算法密碼服務，AES 加密存儲效能可達 10 MB/s。因應趨勢也提供愈來愈多密碼貨幣所採用的 EdDSA 數位簽章算法 (2020 年由 NIST 宣布成為新一代數位簽章標準 FIPS186-5)。

產品規格

實體安全

CC EAL5+ Security chip

密碼算法與功能

Message digest : SHA-2, SHA-3, HMAC

RSA 2048, 4096

ECC with prime-field curves (up to 521 bits) and Edward curve

ECC protocols : ECDSA,ECDH

AES modes : ECB, CBC

Random number generation : AIS-31 (class PTG2) certified

TRNG with NIST SP800-90A Hash-DRBG

API

PKCS#11

Native API

應用實例

聯網安全認證

此安全認證機制可使用於韌體 OTA 升級、參數更新、設備管理等應用。提供物聯網裝置端及行動裝置端密碼服務，若要啟用裝置需經過公鑰認證或金鑰密碼驗證，以此排除聯裝置被偽冒與挾持網的風險。

機密資料加密與存儲

VeloCrypt 擁有彈性的空間規畫，可設定一般磁區與加密磁區，加密磁區需通過認證才能使用。採用可客製化的硬體密碼引擎，提供安全高效之加解密服務，確保資料連線與離線存取之安全性。一般市面上以軟體設計為架構之產品，面對駭客攻擊無法完全防護；而少數選用安全晶片的相似硬體架構產品，效能又無法滿足資料順暢營運的需求。VeloCrypt 兼具高速的加密存儲速度，及安全晶片之硬體架構下的完美防護，保障使用者在不犧牲效能的情況下也能擁有完美硬體安全。

點對點安全通訊

VeloCrypt 兼具高速效能與安全，擁有相當大的彈性與靈活。相較於有一定的漏洞與風險、以軟體為基礎之加密通訊，VeloCrypt 以硬體為防護基礎，強化使用者抵禦竊聽及防竄改的能力，確保資料於不同協定之下的傳輸安全性。而針對市面上現有知名的安全通訊軟體如 Telegram 與 Signal，VeloCrypt 更可進一步依據其應用協議進行客製化，以達相容性並兼具安全性，使任何平台、裝置皆能快速導入 VeloCrypt 的解決方案，減少整體營運成本與時間成本。

密碼貨幣安全交易防護

VeloCrypt 支援密碼貨幣之私鑰儲存與交易簽章等功能，可直接與手機綁定，使其本身成為硬體錢包，無需讀卡機或額外設備。在安全方面，使用通過 CC EAL 5+ 認證的高規格安全晶片，確保私鑰不外洩，有效防護旁通道攻擊及逆向工程。

傳輸介面

Fully compliant with SD3.0 (UHS-I) and SD2.0 specifications

Fit micro SD card dimension

MLC NAND Flash/ SLC NAND Flash

容量

512MB/8GB/32GB

功耗

Working mode : 160mA +35mA

Idle mode : 80mA + 15mA

Sleep mode : 23mA+ 5mA

溫度

Storage temperature : -40"C ~ 125*C

Operation temperature : 0 "C~70"C

註 : 實際下單規格依最新資訊並按照客戶需求調整後規格為準。

靈活隨想、快速實現

VeloCrypt 彈性硬體架構設計，允許所有演算法和標準演算法的客製化，能快速實作於您的系統中，無需額外硬體升級與修改。匯智安全也提供專業服務幫助客戶在 VeloCrypt 上自行客製化非對稱式演算法、硬體密碼引擎、硬體加速功能。面對未來將成真的量子電腦威脅，我們致力於掌握後量子密碼實作及相關演算法的硬體防護，為 VeloCrypt 匯聚尖端技術能量，盼能滿足客戶長期資安需求。

Contact us
WiSECURE Technologies Corporation
4F., No. 218, Sec. 6, Roosevelt Rd., Wenshan Dist.,
Taipei City 116, Taiwan R.O.C.
+886-2-29343166
support@wisecure-tech.com

wisecuretech