SafeNet | THE DATA PROTECTION COMPANY

PS HSM 硬體安全模組

產品簡介

PS HSM (Hardware Security Module)是一款通過 FIPS 140-2 level3 認證之硬體安全模組，內含 4MB secure memory 將所有金鑰存放於硬體模組內部以確保金鑰安全，提供敏感性資料加/解密、簽/驗章等功能，硬體能強化金鑰存儲安全性，防止竄改、竊取。
應用範疇：金融交易(銀行、證券、保險、電子錢包/票證與第三方支付)、雲端資料安全。

高安全性

PS HSM 通過國際標準 FIPS 140-2 level3 認證，當內建 HSM 模組被拔除時，提供金鑰一次性/永久/立即抹除金鑰等功能，防止金鑰被非法竊取，為此強化設備本機安全，防止金鑰被非法盜取，同時**符合法規-PCIDSS 支付卡行業資料安全標準(3.0)** 。

- PCIDSS (3.0) 條文：3.5.2 Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. Within a secure cryptographic device (such as a HSM). (強化金鑰儲存要求與加密資料與加密金鑰分開存放安全性)。

標準演算法&客製化程式(FM)

採標準 PKCS #11，提供 C 、Java 、CAPI 等 API 供開發人員使用，內建真亂數隨機產生器(True Random Number Generator)增加金鑰破解難度，可自行設計演算法，將程式碼載入 HSM 內 Firmware (FM)，保護演算過程安全，防止逆向工程，暴力破解，金鑰(Key)演算均在 HSM 中，能有效分擔伺服器 CPU 的負擔，常見應用 OTP 演算法，演算法於 HSM 運算及驗證，僅回覆認證成功或失敗，有效防止演算法複製、外洩。

負載平衡&高可用性(WLD /HA)

各 AP 程式可透過原廠工具建立虛擬 Slot (WLD- Work Load Distribution 功能)，進行交易隨機分配於不同台 HSM 中，各 AP 作業採獨立，不因 L4 Switch 而導致交易中止無法運行；內建重新連線(HA-High Availability 功能)，能讓網路瞬斷導致 HSM 斷線，HA 能自動重新連線，前端 AP 不需重啟，方便管理者維運、管理。

功能效益

安全性

- 真亂數隨機產生器(True RNG)
- 智慧卡（M of N）金鑰備份
- 雙熱插拔備援電源供應器

效能

- 雙重 LAN
- 每秒最高可達 50/200/1500 次 RSA 簽章速度
- 負載平衡&高可用性（WLD/HA）
- 多執行緒 API

選項模組

- IC 晶片卡開機登入（M of N）模組

簡易管理

- 中文金鑰管理系統-PSK

- HSM 監控儀表板-PSM

【產品型號與效能】

Operation	Data Size (Bytes)	Metric	PL1500	PL220	PL25
RSA sign 1024-bit	16	operations/second	1685.26	369.81	65.00
RSA sign 2048-bit	16	operations/second	695.63	100.18	30.05
RSA sign 4096-bit	16	operations/second	103.08	17.00	10.18
RSA verify 1024-bit	16	operations/second	2321.22	600.85	180.21
RSA verify 2048-bit	16	operations/second	2234.23	600.66	132.00
RSA verify 4096-bit	16	operations/second	1984.29	548.89	4.09

1. 支援作業系統：WIN 2008 R2 (64-bits)、WIN 2012 R2 (64-bits)、WIN 7(32-bits,64-bits)、Solaris 10,11 SPARC (64-bits)、Linux SuSE 12(64-bits)、AIX 6.1(64-bits)、RedHat Enterprise Linux 6 (32-bits,64-bits)。
2. 硬體安控模組需通過 FIPS 140-2 Level 3 認證，具有防止盜取資料之金鑰自動銷毀功能（Tamper protected physical HSM Security）並可配合 PCI 匯流排卡片偵測方式確保硬體安控模組遭受物理攻擊時可自動銷毀金鑰。
3. 內含硬體亂數產生器(True RNG)。
4. 設備使用 TCP/IP 通訊方式與主機連接。
5. 支援標準軟體開發環境： PKCS#11 API、Java JCE/JCA Provider、Microsoft CryptoAPI 與 Firmware 開發工具，可自行客製化 HSM 功能。
6. 不限制硬體密碼模組連線數，無 license 限制。提供連線 Unlimited license（含以上）之原廠證明。
7. 支援對稱式密碼演算法：AES、DES、3DES、CAST-128、RC2、RC4、SEED 和 ARIA，模式支援 ECB、CBC、OFB64 和 CFB-8(BCF)。
8. 支援非對稱式密碼演算法：RSA(長度可達 4096 bits)、DSA、ECDSA、Diffie Hellman (DH) 和 ECC。
9. 硬體密碼模組內含 4MB secure memory 將所有金鑰存放於硬體模組內部以確保金鑰安全，同時支援 External Key Storage 模式，將金鑰透過 KeK 方式存放於外部硬碟需無金鑰儲存總數限制，以符合管理與儲存大量金鑰需求。
10. 提供指令介面(CMD line interface)與圖形化介面(GUI HSM admin interface)之 HSM 管理程式，供遠端電腦進行管理。
11. 內建雙熱插拔備援電源供應器(Redundant power supply)。
12. 支援 PSM(ProtectServer Monitor)中文監控儀表板監控 HSM 設備狀態。
13. SafeNet 原廠教育訓練證明書。

PAYSECURE
TECHNOLOGY

聯絡我們
聯宏科技股份有限公司
聯絡方式
www.paysecure.com.tw
+886-2-2657-1187
support@paysecure.com.tw