

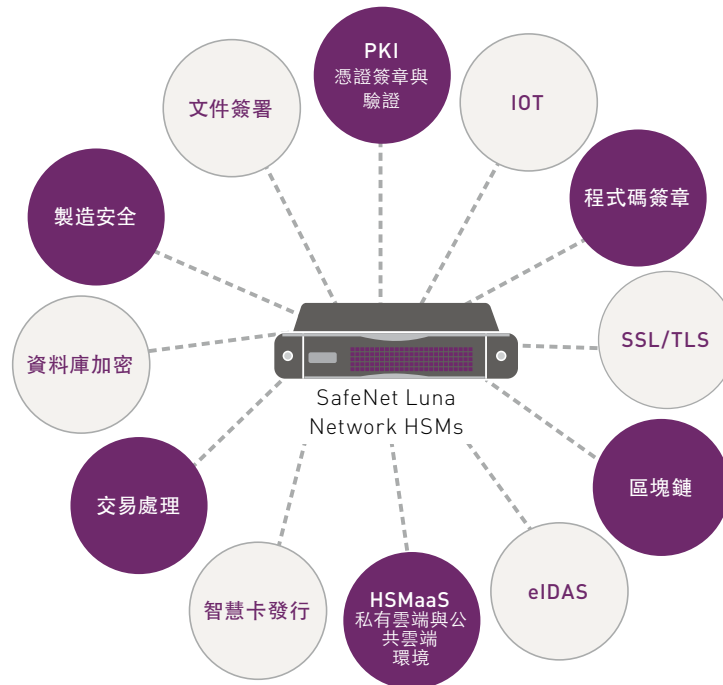
產品簡介

SafeNet Luna Network HSM



以SafeNet Luna Network 硬體安全模組(HSMs)儲存、保護並管理加密金鑰，藉此確保您的機敏資料和重要應用程式之安全。SafeNet Luna Network 硬體安全模組為具高信賴度、防竄改功能之網路型裝置，提供領先市場的優異效能。

請聯繫我們，了解如何將SafeNet Luna Network 硬體安全模組(HSMs)與各類應用程式整合，以加速密碼運算、確保加密金鑰生命週期，並為整體加密架構提供信任根(a root of trust)。



不可不知的產品特色：

優異性能：

- > 市場上最快速之HSM，於高性能使用案例中，運算速度每秒超過20,000次ECC及10,000次RSA。
- > 更低之延遲性可提升效率

最高安全性&合規性：

- > 金鑰永久保存於經FIPS認證，且具防竄改功能之硬體中
- > 符合GDPR、eIDAS、HIPAA、PCI-DSS等法規要求
- > 符合雲端業界標準
- > 多重角色可實現高度分工
- > 多人MofN與多因子身分驗證，提升安全性
- > 安全之稽核紀錄
- > 安全傳輸模式提供高保障傳遞
- > 透過外部量子隨機數生成器[Quantum RNG]生成亂數，提供高品質金鑰

降低成本&省時：

- > 遠端管理HSMs-不需移動
- > 降低稽核與合規之成本和負擔
- > 自動化企業系統，透過REST API管理HSMs
- > 多個應用程式或租戶共享 HSMs，有效管理資源
- > 靈活的分區策略，滿足您對金鑰管理與合規性之需求

技術規格

支援之作業系統

- > Windows, Linux, Solaris, AIX
- > 虛擬: VMware, Hyper-V, Xen, KVM

支援API

- > PKCS#11、Java (JCA/JCE)、Microsoft CAPI與CNG、OpenSSL
- > 使用REST API管理

加密

- > 支援完整Suite B
- > 非對稱: RSA、DSA、Diffie-Hellman、Elliptic Curve Cryptography (ECDSA、ECDH、Ed25519、ECIES) 搭配特定、使用者定義與Brainpool曲線、KCDSA以及更多
- > 對稱: AES、AES-GCM、Triple DES、DES、ARIA、SEED、RC2、RC4、RC5、CAST以及更多
- > 雜湊/訊息摘要/HMAC: SHA-1、SHA-2、SM3以及更多
- > 金鑰衍生: SP800-108 計數器模式
- > 金鑰包裝: SP800-38F
- > 隨機亂數生成: 使用硬體基礎(HW based)真實噪音源與合於NIST 800-90標準之CTR-DRBG, 達成符合AIS 20/31至DRG.4標準之設計。

安全認證

- > FIPS 140-2 Level 3 – 密碼與多因子 (PED)
- > eIDAS CC EAL4+ (AVA_VAN.5 和 ALC_FLR.2) 對應 Protection Profile 419221-5 *

主機介面

- > 端口綁定之4 Gigabit乙太網路端口
- > IPv4和IPv6

物理特性

- > 標準1U 19吋機架式裝置
- > 尺寸: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- > 重量: 28lb (12.7kg)
- > 輸入電壓: 100-240V、50-60Hz
- > 功耗: 最大110W, 一般84W
- > 散熱: 最多每小時376BTU, 一般每小時287BTU
- > 溫度: 運轉 0° C – 35° C、儲存 -20° C – 60° C
- > 相對溼度: 5%至95% (38° C) 非冷凝

安全& 環境合規

- > UL, CSA, CE
- > FCC, CE, VCCI, C-TICK, KC Mark
- > RoHS2, WEEE
- > TAA

可靠性

- > 雙重熱插拔電源
- > 可現地維修零組件
- > 平均失效間隔時間(MTBF)171,308小時

管理& 監控

- > HA災難復原
- > 備份和還原
- > SNMP, Syslog

* 待定

產品系列

HSMs共有兩個系列,每一系列各有3種不同型號,您可依需求從中選擇。

Luna A系列: 密碼驗證, 便於管理。

A700	A750	A790
2 MB 記憶體 分割區: 5 最大分割區數: 5	16 MB 記憶體 分割區: 5 最大分割區數: 20	32 MB 記憶體 分割區: 10 最大分割區數: 100
標準性能: <ul style="list-style-type: none">> RSA-2048: 1,000 tps> ECC P256: 2,000 tps> AES-GCM: 2,000 tps	企業級性能: <ul style="list-style-type: none">> RSA-2048: 5,000 tps> ECC P256: 10,000 tps> AES-GCM: 10,000 tps	最大性能: <ul style="list-style-type: none">> RSA-2048: 10,000 tps> ECC P256: 22,000 tps> AES-GCM: 17,000 tps

Luna S系列: 多因子 (PED) 驗證, 滿足高保證使用需求。

S700	S750	S790
2 MB 記憶體 分割區: 5 最大分割區數: 5	16 MB 記憶體 分割區: 5 最大分割區數: 20	32 MB 記憶體 分割區: 10 最大分割區數: 100
標準性能: <ul style="list-style-type: none">> RSA-2048: 1,000 tps> ECC P256: 2,000 tps> AES-GCM: 2,000 tps	企業級性能: <ul style="list-style-type: none">> RSA-2048: 5,000 tps> ECC P256: 10,000 tps> AES-GCM: 10,000 tps	最大性能: <ul style="list-style-type: none">> RSA-2048: 10,000 tps> ECC P256: 22,000 tps> AES-GCM: 17,000 tps

tsp = 每秒鐘交易量

與我們聯絡: 如需所有辦公室位置和聯繫資訊, 請造訪 safenet.gemalto.com

跟隨我們: blog.gemalto.com/security

 GEMALTO.COM


security to be free