Product Brief

THALES
CYBERSECURITY

Luna Network HSM

cpl.thalesgroup.com

透過 Thales Luna 網路硬體安全模組 (HSM) 儲存、保護和管理您的加密金鑰，確保您的機敏資料和關鍵應用程式的安全。 Luna 網路硬體安全模組是高可靠性、防篡改的網路連接設備，提供業界領先的效能和加密靈活性。
與我們聯繫，了解如何將 Luna Network HSM 整合到各種應用程式中，加速加密操作、保障加密金鑰的生命週期安全，爲您的整個加密基礎架構提供信任根。

What you need to know:

卓越性能：

- 滿足您的高吞吐量需求，每秒可執行超過 20,000 次 ECC 運算和 10,000 次 RSA 運算，適用於高效能應用場景
- 更低的延遲，提升效率

最高安全性和合規性：

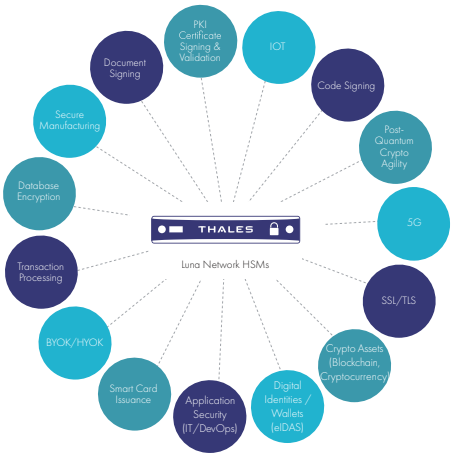
- 金鑰儲存方式通過 FIPS 驗證、防竄改硬體
- 滿足 GDPR、eIDAS、HIPAA、PCI-DSS 等合規性要求
- 業界公認的雲端標準
- 多角色配置，實現嚴格的職責分離
- MofN多人特徵控制及多因素驗證，提升安全性
- 安全的稽核日誌記錄
- 安全的傳輸模式，確保高可靠性交付
- 提供強大金鑰，支援內外部雙重熵來源，並與關鍵主流 QRNG 供應商整合
- 使用 Luna Backup HSM 在硬體中安全地備份和複製金鑰，或使用 Data Protection on Demand 將金鑰備份到雲端，以實現冗餘、可靠性和災難復原

降低成本，節省時間：

- 遠端管理 HSM - 無需奔波
- 降低審計和合規成本及負擔
- 透過 REST API 實現企業系統自動化，管理 HSM
- 透過在多個應用程式或租用戶之間共用 HSM，高效管理資源
- 靈活的分區策略，滿足您的金鑰管理和合規需求
- 在容器中使用 Luna Client，可提升可攜性、提高效率並減少額外負擔
- 功能模組
  - 擴充原生 HSM 功能
  - 在 HSM 的安全性規範內開發和部署自訂程式碼

以環境爲核心的設計

Thales Luna HSM 採用環保設計 (eco-design)，致力於在每一代產品中實現可量化且顯著的碳足跡減少，同時降低電力消耗與營運成本。這些努力與 Thales 的 ESG (環境、社會與公司治理) 承諾一致，攜手打造更綠色且更安全的世界。



技術規格

支援的作業系統

- Windows、Linux、Solaris、AIX
- 虛擬機器：VMware、Hyper-V、Xen、KVM

API Support

- PKCS#11、Java (JCA/JCE)、Microsoft CAPI 與 CNG、OpenSSL
- 用於管理的 REST API

密碼學

- Luna PQC 功能模組中的後量子機制
- PQC 演算法 : HSS/LMS、ML-KEM (FIPS 203)、ML-DSA (FIPS 204)
- 完全支援 Suite B
- 支援 CNSA 2.0
- 非對稱加密：RSA、DSA、Diffie-Hellman、橢圓曲線密碼學 (ECDSA、ECDH、Ed25519、ECIES)，支援命名曲線、使用者自訂曲線和 Brainpool 曲線，KCDSA、SM2 等
- 對稱加密：AES、AES-GCM、Triple DES、DES、ARIA、SEED、RC2、RC4、RC5、CAST、SM4 等
- 雜湊/訊息摘要/HMAC：SHA-1、SHA-2、SHA-3、SM3 等
- 金鑰派生：SP800-108 計數器模式
- 金鑰封裝：SP800-38F
- 隨機數產生：採用基於硬體的眞噪音源，並結合符合 NIST 800-90A 的 CTR-DRBG，整體設計符合 AIS 20/31 DRG.4 要求

- 數位錢包金鑰管理：BIP32 / SLIP10

5G加密機制包括：
- 使用者驗證：Milenage、Tuak 和 COMP128
- 使用者隱私保護：ECIES

安全認證
- FIPS 140-2 3級驗證 – 密碼與多因素身份驗證 (PED)
- FIPS 140-3 3級驗證 – 密碼與多因素身份驗證 (PED)
- 符合通用準則 EAL4+ (AVA_VAN.5 和 ALC_FLR.2) 標準，並已通過 EN 419 221-5 保護設定檔認證
- 符合 eIDAS 標準的合格簽名或印章創建設備 (QSCD) 認證
- 巴西 INMETRO 認證 (原 ITI)
- 新加坡 NITES 通用準則方案

主機介面
- IPv4 和 IPv6
- 連接埠綁定
  2 種選項
  - 4 個 1G RJ45 乙太網路連接埠 (所有裝置預設配置)
  - 2 個 10G SFP+ 連接埠用於光纖網路連接，以及 2 個 1G 連接埠 (僅限 790 型號)

實體規格
- 標準 1U 19 吋機架式設備
- 尺寸：19" x 21" x 1.725" (482.6 mm x 533.4mm x 43.815mm)
- 重量：28 磅 (12.7 公斤)
- 輸入電壓：100-240V，50-60Hz
- 耗電量：最高 110W，一般 84W
- 散熱性：最高 376 BTU/小時，一般 287 BTU/小時
- 溫度：作業溫度 0°C 至 35°C，存放溫度 -20°C 至 60°C
- 相對濕度：5% 至 95% (38°C 時無冷凝)

安全與環境合規認證
- 80 PLUS 銀級認證
- UL、CSA、CE
- FCC、CE、VCCI、C-TICK、KC Mark
- RoHS2、WEEE
- TAA
- 印度 BIS [IS 13252 (Part 1)/IEC 60950-1]

可靠性
- 雙熱插拔電源
- 可現場維修的組件
- 平均故障間隔時間 (MTBF) 171,308 小時

管理與監控
- 高可用性故障轉移/負載平衡
- 硬體備份與恢復，支援本地或雲端硬體
- SNMP、Syslog

可用型號

Luna Network HSM 提供兩個系列，每個系列包含 3 種不同型號，可滿足您的各種需求。

Luna A 系列：

密碼認證，方便管理

標準型效能 A700	企業級效能 A750	最高效能 A790
最高 4 MB 記憶體	最高 32 MB 記憶體	最高 64 MB 記憶體
分區數：5	分區數：5	分區數：10
最大分區數：5	最大分區數：20	最大分區數：100
效能：	**效能：**	**效能：**
RSA-2048: 1,000 tps	RSA-2048: 5,000 tps	RSA-2048: 10,000 tps
ECC P256: 2,000 tps	ECC P256: 10,000 tps	ECC P256: 22,000 tps
AES-GCM: 2,000 tps	AES-GCM: 10,000 tps	AES-GCM: 17,000 tps

Luna S 系列：

適用於高可靠性用例的多因素 (PED) 身份驗證。

標準型效能 S700	企業級效能 S750	最高效能 S790
最高 4 MB 記憶體	最高 32 MB 記憶體	最高 64 MB 記憶體
分區數：5	分區數：5	分區數：10
最大分區數：5	最大分區數：20	最大分區數：100
效能：	**效能：**	**效能：**
RSA-2048: 1,000 tps	RSA-2048: 5,000 tps	RSA-2048: 10,000 tps
ECC P256: 2,000 tps	ECC P256: 10,000 tps	ECC P256: 22,000 tps
AES-GCM: 2,000 tps	AES-GCM: 10,000 tps	AES-GCM: 17,000 tps

tps = transactions per second

THALES

CYBERSECURITY

聯絡我們

所有辦公室地點與聯絡資訊請參訪:

cpl.thalesgroup.com/contact-us

cpl.thalesgroup.com