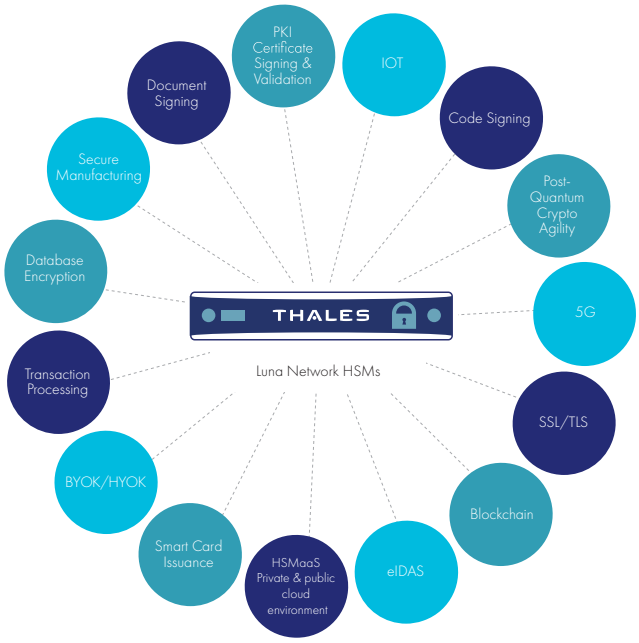
cpl.thalesgroup.com

Thales Luna Network HSM

在 Thales Luna Network 硬體安全模組（HSM）中儲存、保護和管理您的金鑰，可保障您的機敏資料和重要應用程式的安全 – 提供高安全性、防竄改、網路連結功能，效能領先業界。

請聯絡我們以瞭解 Luna Network HSM 如何整合各種應用程式來加速加密作業、保障金鑰週期安全、為整體加密設計最安全的信任基礎架構。



重點資訊：

卓越效能：

- 超過每秒 20,000 ECC 和 10,000 RSA 作業的高效運行，符合您高效能的需求
- 延遲時間更短，效能更高

最高的安全性與合規規格：

- 金鑰儲存方式通過 FIPS 驗證、防竄改硬體
- 符合GDPR、eIDAS、HIPAA、PCI-DSS 等合規要求
- 雲端現存標準
- 多角色管理，分工分權
- MofN多人特徵控制及多因素驗證，提升安全性
- 確保稽核記錄安全性
- 具備安全傳輸模式的高保證度傳遞效能
- 以外部 Quantum RNG 植入的高品質金鑰
- 使用Luna backup HSM安全地備份和複製硬體中的金鑰，或根據需要使用資料保護將金鑰備份和複製到雲，以實現冗餘、可靠性和災難恢復

降低成本並節省時間：

- 遠端管理 HSM – 無需奔波
- 減少稽核與合規開銷負擔
- 企業系統自動化，透過 REST API 管理 HSM
- 多應用程式或租戶中分享HSM，有效管理資源
- 彈性分割區規則，符合您的金鑰管理與合規需求
- 使用 SafeNet Luna Client 作為容器，攜帶更容易、效率更高、經常性開銷更低
- 功能模組
  - 延伸原生 HSM 功能
  - 於 HSM安全規範中建立和部署客製化程式

技術規格

支援作業系統

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

支援應用程式編程介面

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

加密

- 完整支援 Suite B
- 非對稱式演算法：RSA、DSA、Diffie-Hellman、Elliptic Curve 加密演算法（ECDSA、ECDH、Ed25519、ECIES），搭配命名、使用者自訂和 Brainpool curves、KCDSA 等
- 對稱式演算法：AES、AES-GCM、Triple DES、DES、ARIA、SEED、RC2、RC4、RC5、CAST 等
- 雜湊／訊息摘要／HMAC：SHA-1, SHA-2, SHA-3, SM2, SM3, SM4等
- Key Derivation：SP800-108 Counter Mode
- Key Wrapping：SP800-38F
- Random Number Generation：設計符合 AIS 20/31 對 DRG.4 使用以硬體為基礎的真雜訊來源，並配合 NIST 800-90A 相容 CTR-DRBG
- Digital Wallet Encryption：BIP32
- 用於用戶身份驗證的5G加密機制：Milenage、Tuak和COMP128

安全憑證

- FIPS 140-2 Level 3 – 密碼與多因素驗證（PED）
- 針對保護規範EN 419 221-5的通用標準EAL4 +（AVA_VAN.5和ALC_FLR.2）
- 符合eIDAS要求的合格簽名或印章創建設備（QSCD）清單
- 新加坡NITES通用標準計劃*

主機介面

- 2個選項：4 Gigabit 具有端口綁定的乙太網路端口，或2個10G光纖網路連接和2個1G帶端口綁定的端口
- 支援IPv4和IPv6

實體規格

- 標準 1U 19 英吋機架式規格
- 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 376BTU／小時，一般287BTU／小時
- 溫度：作業溫度 0° C – 35° C，存放溫度-20° C – 60° C
- 相對溼度：5% 至 95%（38° C）非冷凝

安全性與環境合規性

- UL, CSA, CE
- FCC, CE, VCCI, C-TICK, KC Mark
- RoHS2, WEEE
- TAA
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

可靠性

- 雙熱插拔電源
- 可現場維修模組化組件
- 平均故障間隔（MTBF）171,308 小時

管理及監控

- HA 災難修復
- 將硬體備份和復原到本地或雲中的硬體
- SNMP、Syslog

* 評估中

供應機型

Luna Network HSM 兩大系列各有 3 種不同機型供您選擇，符合您需求。

Luna A 系列：

密碼驗證，簡易管理。

標準效能 **A700**	企業效能 **A750**	最大效能 **A790**
2 MB 記憶體	16 MB 記憶體	32 MB 記憶體
Partitions: 5	Partitions: 5	Partitions: 10
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
效能： RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**效能：** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**效能：** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

Luna S 系列：

多因素（PED）驗證，安全性更高。

標準效能 **S700**	企業效能 **S750**	最大效能 **S790**
2 MB 記憶體	16 MB 記憶體	32 MB 記憶體
Partitions: 5	Partitions: 5	Partitions: 10
Maximum Partitions: 5	Maximum Partitions: 20	Maximum Partitions: 100
效能： RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**效能：** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**效能：** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

tps = 每秒交易處理量

關於 Thales

不論任何企業在個資保護的技術上都透過Thales保護他們的資料。在資料安全方面，企業面臨著越來越多的決定性時刻。無論是建置加密策略，移轉到雲端還是滿足合規性要求，在邁向數位化轉型時，您可以依靠Thales來保護您的有價資料。

關鍵時刻，關鍵技術