

Luna 8 Network HSM

數位信任的基礎



Luna 8 Network HSM 全新推出

以量子安全信任根為基礎，提供可擴充、多租戶、高效能且可靠的安全防護

使用 Luna 網路硬體安全模組 (HSM) 保護您的機敏資料、身分和關鍵應用程式。專為安全儲存、保護及管理加密金鑰而設計，具備高安全保障、量子安全與防竄改特性，提供可擴充的多租戶安全防護，以及業界領先的效能，滿足後量子密碼學 (PQC) 工作負載需求。Luna 8 搭載 Thales 自行設計的加密處理器，具備高資料處理量、強大的安全隔離能力，以及所需的密碼敏捷性 (Crypto Agility)，協助企業快速因應不斷變化的業務需求、新興威脅與新型加密演算法。

與我們聯繫，了解 Luna Network HSM 如何協助您加速整合、以硬體保護整個加密金鑰生命週期，並簡化合規管理。Luna Network HSM 支援廣泛的應用程式，協助企業建立量子安全信任根，全面保護加密基礎架構，並為未來的安全需求做好準備。

最高安全與合規性

- 金鑰始終保存在防篡改硬體中
- 設計符合 GDPR、eIDAS、HIPAA、PCI-DSS 等合規性要求
- 多角色設計，實現嚴格的職責分離
- 採用 MofN 與多重因素身分驗證進行仲裁授權，以提升安全性
- Thales 自行設計加密處理器的側信道防護
- 透過設備認證確保高可靠性交付
- 板載雙熵源（包括 QRNG）並支援外部熵源
- 透過 Luna Backup HSM 在硬體中安全備份金鑰，提升備援能力、可靠性與災難復原能力

擴展規模並優化營運成本

- 每個 Thales HSM 可包含一個或兩個加密模組；每個加密模組獨立運行，在相同的機架空間內實現雙倍密度
- 每個加密模組最多可託管 15 個 HSM 用例，因此，當配置兩個加密模組時，每個裝置最多可支援 30 個 HSM 用例
- 在同一硬體上的安全容器中執行多個 Luna 8 韌體版本
- 透過 API 和 CLI 工具實現 HSM 管理和作業流程的自動化
- 與現有 IT 基礎架構工具整合，用於監控、日誌記錄和指標管理
- 頻外診斷與硬體使用率指標；靈活的安全策略，滿足您的金鑰管理和合規性需求
- 使用容器中的 Luna Client，可提高可移植性、效率並降低開銷



環保設計

Thales HSM 透過生態設計，顯著降低了碳足跡。秉承 Thales 的 ESG（環境、社會和治理）承諾，Luna 8 的單筆交易能源效率比 Luna 7 高出 20 倍。

技術規格

支援的作業系統

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

API 支援

- PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL
- 用於管理的 API

後量子密碼學 (PQC)

- ML-KEM (FIPS 203 金鑰封裝) 和 ML-DSA (FIPS 204 數位簽章)
- 狀態式雜湊簽章 (Stateful Hash-Based Signatures) : LMS 和多層 HSS (RFC 8554 / NIST SP 800-208)

橢圓曲線密碼學 (ECC)

- 經 FIPS NIST 認證的質數曲線 (P-192、P-224、P-256、P-384、P-521) 和 Brainpool 曲線 (P192 至 P512)，適用於 ECDSA/ECDH 和 ECIES
- Koblitz 曲線 (secp256k1)，適用於 BIP32 分層確定性錢包金鑰管理
- Montgomery 曲線 (X25519、X448) 與 Edwards 曲線 (Ed25519、Ed448)

非對稱加密和對稱加密

- 非對稱加密：RSA (金鑰長度最高可達 4096 位元)，支援標準 PKCS#1 v1.5、OAEP 和 FIPS 認證的 PSS 機率簽章生成
- 對稱加密：AES (128 位元、192 位元、256 位元)，支援 ECB、CBC、CBCPAD、CTR、GCM、GMAC、金鑰封裝和 512 位元 AES-XTS 模式。ARIA、SEED
- 傳統加密：三重 DES (3DES) CBC/ECB 僅保留用於向後相容的解封裝/解密

安全雜湊、金鑰衍生函數 (KDF) 和電信

- SHA-2 和 SHA-3 安全雜湊 (224 至 512 位元) 和 HMAC
- SHAKE-128、SHAKE-256 可延伸輸出函數 (XOF)
- 金鑰派生：NIST SP 800-108 計數器模式
- 金鑰封裝：NIST SP 800-38F
- 3GPP 行動通訊蜂窩安全性：MILENAGE、TUAk 和 COMP128 使用者認證設定檔

數位錢包與區塊鏈託管

- BIP32 與 SLIP10 分層確定性 (HD) 金鑰管理

隨機數生成

- 採用硬體級真噪聲源，並結合符合 NIST 800-90A 標準的 HMAC_DRBG，設計符合 AIS 20/31 至 DRG.4 標準

安全認證

- FIPS 140-3 3 級*
- 符合通用準則 EAL4+ (AVA_VAN.5 和 ALC_FLR.2) EN 419 221-5 保護設定檔認證*
- 符合 eIDAS 2 標準的合格簽名或印章創建設備 (QSCD) 認證*

網路

- 4 個 10G SFP+ 端口，支援多模或單模光纖和 RJ45 銅纜
- IPv4、IPv6*、連接埠綁定*
- 1 個 1G RJ45 乙太網路端口，用於連接基板管理控制器 (BMC)

物理特性

- 標準 1U 19 吋機架式設備
- 尺寸：
 - 17.44 英吋 (寬) x 21.95 英吋 (深) x 1.71 英吋 (高)
 - 443 毫米 (寬) x 557.6 毫米 (深) x 43.5 毫米 (高)
- 重量：
 - 單模組設備 26.5 磅 (12 公斤)
 - 雙模組設備 30 磅 (13.6 公斤)
- 輸入電壓：100-240 伏特交流電，50-60 赫茲
- 典型功耗：
 - 單模組設備 ~ 135 瓦
 - 雙模組設備 ~ 270 瓦
- 最大耗電量：
 - 單模組設備 ~ 225 瓦
 - 雙模組設備 ~ 450 瓦
- 溫度：工作溫度 0°C – 40°C，儲存溫度 -20°C – 60°C
- 相對濕度：5% 至 95% (38°C) 無冷凝

安全與環境合規

- 80 PLUS 白金認證
- UL, CSA, CE
- FCC, CE
- RoHS3, WEEE
- TAA
- 印度 BIS [IS 13252 (Part 1)/IEC 60950-1]*

可靠性

- 雙熱插拔電源和風扇
- 平均故障間隔時間 (MTBF)
 - 單模組設備：289,444
 - 雙模組設備：171,236

管理與監控

- 量子安全高可用性故障轉移 / 負載平衡
- 量子安全硬體到硬體的備份與恢復
- rsyslog 和 BMC 用於帶外診斷

* In process



可用的 Luna 網路 HSM 型號

型號			
	Luna 100 (標準性能)	Luna 150 (企業級效能)	Luna 190 (最高性能)
容器數量	1	Up to 6	Up to 15
金鑰儲存	128 MB	1024 MB	4096 MB

Luna 8 網路 HSM 根據效能、金鑰容量和支援的容器類型提供三種型號。每種型號都針對常見的部署需求量身定制，方便您為自身環境選擇合適的解決方案。每個安全容器都託管一個獨立的 Luna 8 HSM 實例，並支援最多 10 個分區。

關於 Thales

Thales 是網路安全領域的全球領導者，致力於幫助企業、政府和全球最值得信賴的組織，以最高的投資報酬率，大規模地保護關鍵應用程式、機敏資料、身分和軟體。我們擁有超過 30,000 家客戶，其中包括 58% 的《財富》世界 500 強企業，我們的解決方案已部署在全球 148 個國家。透過我們創新的服務和整合平台，Thales 幫助客戶更了解風險、抵禦網路威脅、彌補合規漏洞，並每天為數十億消費者提供值得信賴的數位化體驗。