cpl.thalesgroup.com

THALES

Thales Luna PCIe HSM

通過在Thales Luna PCIe HSM(高安全性、防篡改、PCIe卡)中存儲、保護和管理加密金鑰，機敏資料和重要應用程式。為應用程式提供高效能加密處理器的特定存取權限。快速將這種經濟高效的解決方案直接嵌入伺服器和安全設備，從而獲得滿足FIPS 140-2標準的保障。

您需要瞭解的優勢：

卓越效能和易用性

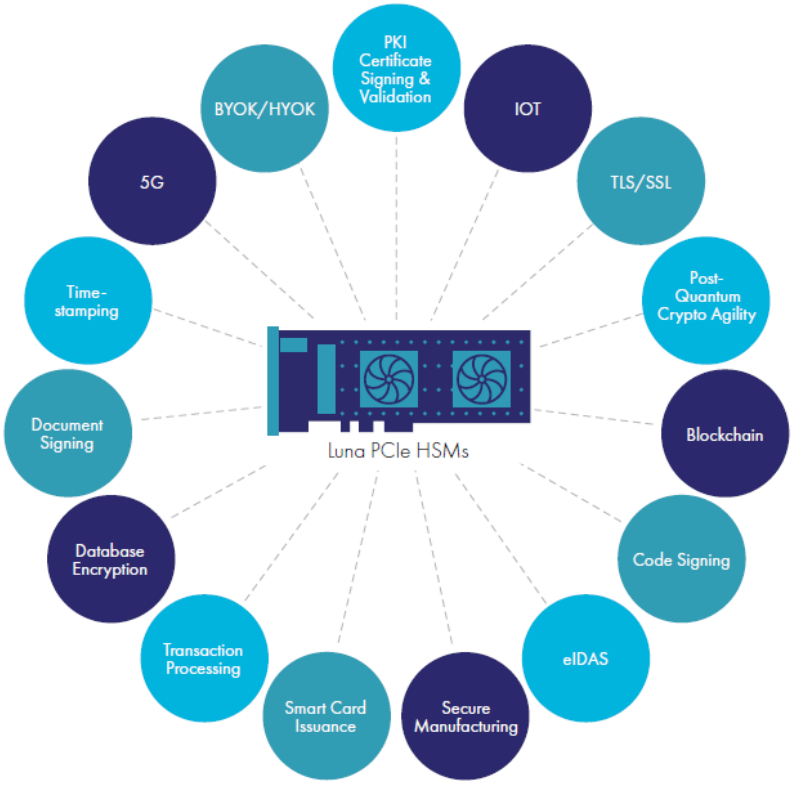
- 對於高效能應用場景，每秒可超過20,000次ECC或10,000次RSA操作，是市場上最快的HSM
- 延遲時間更短，效率更高
- 專用的應用存取權限
- Low profile PCIe卡

功能模組

- 擴展本地HSM功能
- 在HSM的安全範圍內開發和部署自訂代碼

最高的安全性和合規規格

- 金鑰儲存方式通過FIPS驗證、防篡改硬體
- 符合GDPR、eIDAS、HIPAA、PCI-DSS等的合規性要求
- 多重角色以實現分工分權
- MofN多人特徵及多因素認證，提升安全性
- 確保稽核紀錄安全性
- 具備安全運輸模式高保證度傳遞效能



技術規格

支援的作業系統

- Windows, Linux

API支援

- PKCS#11、Java (JCA/JCE)、Microsoft CAPI和CNG、OpenSSL

加密演算法

- 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, ECIES), 包括命名的、使用者自訂曲線以及Brainpool曲線、KCDSA等
- 對稱式演算法：AES、AES-GCM、Triple DES、DES、ARIA、SEED、RCS、RC4、RC5、CAST等
- Hash/Message Digest/HMAC：SHA-1、SHA-2、SM3、SM4等
- Key Derivation：SP800-108 Counter mode
- Key Wrapping：SP800-38F
- 亂數產生：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

安全認證

- FIPS 140-2 Level 3 — 密碼和多因素(PED)認證
- eIDAS CC EAL4+(AVA_VAN.5 和 ALC_FLR.2)， 根據保護設定檔419221-5*

實體規格

- Low profile PCIe卡
- 尺寸：69.6mm x 167mm x 187mm (2.74" x 6.57" x 0.74")
- 耗電量：最高18W，日常14W
- 散熱性：最高61.4BTU/小時，日常47.8BTU/小時
- 溫度：作業溫度0℃ –50℃，存放溫度-20℃ –60℃
- 相對濕度：5% –95% (38℃) 無冷凝

安全和環保合規性

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

主機介面

- PCI-Express CEM 3.0, PCI, PCI Express Base 2.0

可靠性

- 備份/恢復
- 高可用性(HA)
- 平均故障間隔(MTBF) 997,508小時

* 正在評定中

供應機型

Luna PCIe HSM有兩個系列可供選擇，每個都有三種不同的型號可以滿足您的要求。

Luna A系列:

密碼驗證，方便管理。

標準效能： A700	企業效能： A750	最高效能： A790
記憶體: 2MB	記憶體: 16MB	記憶體: 32MB
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)身份驗證，用於需要高可信度的部署環境。

標準效能： S700	企業效能： S750	最高效能： S790
記憶體: 2MB	記憶體: 16MB	記憶體: 32MB
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: 每秒處理次數

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、轉移到雲端還是遵守合規要求，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