プロダクトブリーフ

Luna Network HSM

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

タレスLuna Network HSM（ハードウェアセキュリティモジュール）で暗号鍵を保管、保護、管理することで、機密データや重要なアプリケーションを保護できます。Luna Network HSMは、高保証の、耐タンパ性を備えたネットワーク接続アプライアンスであり、市場で最高クラスのパフォーマンスとクリプトアジリティ（暗号の俊敏性）を提供します。

Luna Network HSMは、広範なアプリケーションに統合でき、暗号処理を加速し、暗号鍵のライフサイクルを保護すると同時に、暗号インフラストラクチャ全体の信頼の基点として機能します。詳細について、ぜひ当社にお問い合わせください。

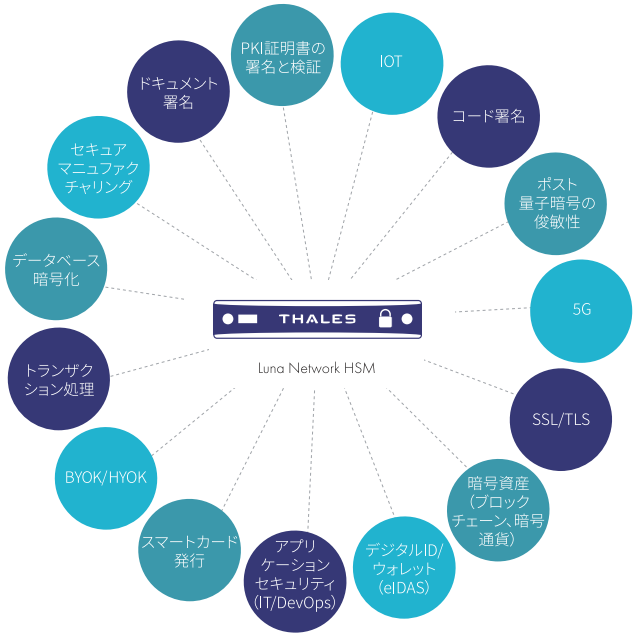
主な機能と利点

優れたパフォーマンス:

- 毎秒20,000以上の楕円曲線暗号と10,000以上のRSA暗号処理で高スループット要件を満たし、高性能ユースケースに対応
- レイテンシを短縮して効率を向上

最高レベルのセキュリティとコンプライアンス:

- 鍵は常にFIPS認証取得済みの耐タンパ性のハードウェアに保管
- GDPR、eIDAS、HIPAA、PCI-DSSなどのコンプライアンス要件に対応
- クラウドのデファクトスタンダード



- 複数の役割を設けることで、強力な職務分掌を実現
- セキュリティを強化する多要素認証を備えたマルチユーザーMofN
- セキュアな監査ロギング
- セキュアな転送モードによる高保証の配信
- 外部のQuantum RNGシードによる高品質な鍵生成
- 鍵は、冗長性、信頼性、ディザスタリカバリを確保するために、Luna Backup HSMを使用してハードウェア内に、またはData Protection on Demandを使用してクラウドに、安全にバックアップと複製が可能

コスト削減と時間短縮

- HSMをリモートで管理 - 出張不要
- 監査とコンプライアンスのコストと負担を軽減
- REST APIによるHSM管理のための企業システムの自動化
- 複数のアプリケーションやテナントでHSMを共有することで、リソースを効率的に管理
- 鍵管理とコンプライアンスのニーズに対応した柔軟なパーティションポリシー
- コンテナ内のLunaクライアントを使用することで、ポータビリティの向上、効率性の向上、オーバーヘッドの削減が可能
- ファンクショナルモジュール
  - ネイティブHSMの機能を拡張
  - HSMの安全な範囲内でカスタムコードの開発と展開が可能

技術仕様

OSサポート

- Windows、Linux、Solaris、AIX
- 仮想: VMware、Hyper-V、Xen、KVM

APIサポート

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

暗号化

- Luna PQCファンクショナルモジュール内のポスト量子暗号メカニズム
- Suite Bの完全サポート
- 非対称: RSA、DSA、Diffie-Hellman、名前付き曲線、ユーザー定義曲線、Brainpool曲線による楕円曲線暗号（ECDSA、ECDH、Ed25519、ECIES）、KCDSAなど
- 対称： AES、AES-GCM、Triple DES、DES、ARIA、SEED、RC2、RC4、RC5、CASTなど
- ハッシュ/メッセージダイジェスト/HMAC：SHA-1、SHA-2、SHA-3、SM2、SM3、SM4など
- 鍵導出: SP800-108カウンターモード
- 鍵ラッピング: SP800-38F
- 乱数生成: NIST 800-90A準拠のCTR-DRBGとともにHWベースのノイズ源を使用して、AIS 20/31からDRG.4に準拠するように設計

- デジタルウォレット暗号化: BIP32
- サブスクライバ認証用の5G暗号化メカニズム: Milenage、Tuak、COMP128

セキュリティ認定
- FIPS 140-2 Level 3認証取得済み – パスワードと多要素(PED)
- FIPS 140-3 Level 3認証取得済み – パスワードと多要素(PED)
- Protection Profile EN 419 221-5に対するコモンクライテリアEAL4+(AVA_VAN.5およびALC_FLR.2)認証取得済み
- eIDAS規則準拠の適格電子署名生成装置(QSCD)のリストに掲載
- シンガポールNITESコモンクライテリアスキーム

ホストインターフェース
- 2つのオプション: ポートボンディング付き4ギガビットイーサネットポート、または10Gファイバーネットワーク接続(x 2)とポートボンディング付き1G(x 2)
- IPv4およびIPv6

物理的特徴
- 標準的な1Uサイズの19インチラックマウントアプライアンス
- 寸法: 19" x 21" x 1.725" (482.6mm x 533.4mm x 43.815mm)
- 重量: 28lb (12.7kg)
- 入力電圧: 100-240V、50-60Hz
- 消費電力: 最大100W、標準84W
- 熱放散: 最大376BTU/時、標準287BTU/時
- 温度: 動作時 0°C～35°C、保管時 -20°C～60°C
- 相対湿度: 5%～95% (38°C) 非結露

安全・環境コンプライアンス
- UL、CSA、CE
- FCC、CE、VCCI、C-TICK、KCマーク
- RoHS2、WEEE
- TAA
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

信頼性
- ホットスワップ対応のデュアル電源
- フィールドサービスの利用が可能なコンポーネント
- 平均故障間隔(MTBF) 171,308時間

管理および監視
- HAディザスタリカバリ
- オンプレミスまたはクラウド上のハードウェアへのバックアップと復元
- SNMP、Syslog

利用可能なモデル

Luna Network HSMには2つのシリーズがあり、各シリーズに用意された3種類のモデルからお客様のニーズに合わせてお選びいただけます。

Luna Aシリーズ:

管理を容易にするためのパスワード認証

標準パフォーマンス A700	エンタープライズパフォーマンス A750	最大パフォーマンス A790
4 MBメモリ	32 MBメモリ	64 MBメモリ
パーティション: 5	パーティション: 5	パーティション: 10
最大パーティション: 5	最大パーティション: 20	最大パーティション: 100
パフォーマンス: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**パフォーマンス:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**パフォーマンス:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

Luna Sシリーズ:

高保証ユースケース向けの多要素(PED)認証

標準パフォーマンス S700	エンタープライズパフォーマンス S750	最大パフォーマンス S790
最大4 MBメモリ	最大32 MBメモリ	最大64 MBメモリ
パーティション: 5	パーティション: 5	パーティション: 10
最大パーティション: 5	最大パーティション: 20	最大パーティション: 100
パフォーマンス: RSA-2048: 1,000 tps ECC P256: 2,000 tps AES-GCM: 2,000 tps	**パフォーマンス:** RSA-2048: 5,000 tps ECC P256: 10,000 tps AES-GCM: 10,000 tps	**パフォーマンス:** RSA-2048: 10,000 tps ECC P256: 22,000 tps AES-GCM: 17,000 tps

tps = 1秒当たりのトランザクション処理件数

cpl.thalesgroup.com

お問い合わせ先 – Email: cpl.jpsales@thalesgroup.com
すべてのオフィスの所在地と連絡先情報につきましては、cpl.thalesgroup.com/contact-usをご覧ください。