

Luna 8

Network HSM

デジタルトラストの基盤



Luna 8 Network HSMのご紹介

拡張性、マルチテナント対応、高いセキュリティ性能と信頼性を備えた量子安全な信頼の基点(Root of Trust)
機密データ、ID、重要なアプリケーションの保護には、Luna Network HSM（ハードウェアセキュリティモジュール）が最適です。Luna Network HSMは、暗号鍵を安全に保管・保護・管理するために設計された、高い信頼性と耐タンパー性を備えた量子安全なアプライアンスです。ポスト量子暗号(PQC)ワークロード向けに、拡張性に優れたマルチテナントセキュリティと市場をリードするパフォーマンスを提供します。タレス独自設計の暗号プロセッサを搭載したLuna 8は、高スループット、強力なセキュリティ分離に加え、クリプトアジリティ(暗号の俊敏性)を提供し、進化するビジネス要件や、新たな脅威、最新の暗号アルゴリズムに迅速に対応できます。

Luna Network HSMが、統合の迅速化、暗号鍵ライフサイクル全体のハードウェアによる保護、コンプライアンス対応の簡素化にどのように役立つかについて、ぜひお問い合わせください。幅広いアプリケーションをサポートするLuna Network HSMは、量子安全な信頼の基点(Root of Trust)を確立し、暗号基盤全体を保護し、将来にわたって安全性を確保します。

最高レベルのセキュリティとコンプライアンス

- 鍵は常に改ざん検知機能を備えたハードウェア内に保持
- GDPR、eIDAS、HIPAA、PCI DSSなどのコンプライアンス要件への対応を考慮して設計
- 強力な職務分掌を実現する複数のロールをサポート
- MofNによるクォーラム認証と多要素認証でセキュリティを強化
- タレス設計の暗号プロセッサに対するサイドチャネル攻撃対策
- デバイスのアテステーションによりHSMの高い信頼性を保証
- オンボードのデュアルエントロピーソース(QRNGを含む)、さらに外部エントロピーソースのサポート
- 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を使用して鍵をハードウェア内で安全にバックアップ

運用コストの最適化と拡張性の向上

- 各HSMには1つまたは2つの暗号モジュールを搭載可能。各暗号モジュールは独立して動作するため、同じラックスペースで2倍の収容密度を実現
- 各暗号モジュールは最大15個のHSMインスタンスをホスト可能。2つの暗号モジュールを搭載した構成では、1台のアプライアンスで最大30個のHSMインスタンスを実行可能
- 同一ハードウェア上のセキュアコンテナ内で、複数のLuna 8ファームウェアバージョンを実行可能
- APIおよびCLIツールを使用して、HSMの管理・運用プロセスを自動化
- 監視・ログ収集・メトリクス取得のために、既存のITインフラストラクチャツールと連携可能
- 帯域外(Out-of-Band)診断およびハードウェア使用率メトリクスを提供
- 鍵管理およびコンプライアンス要件に対応する柔軟なセキュリティポリシー
- コンテナ内のLuna Clientを使用することで、ポータビリティと効率性の向上、オーバーヘッドの削減が可能



環境配慮型の設計

タレスのHSMは、エコデザインを通じて、カーボンフットプリントを測定可能なレベルで大幅に削減しています。タレスのESG(環境、社会、ガバナンス)への取り組みに沿って、Luna 8はLuna 7と比較して、1 トランザクションあたり20倍のエネルギー効率を実現しています。

技術仕様

OSサポート

- Windows, Linux
- 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API

ポスト量子暗号(PQC)

- ML-KEM (FIPS 203 鍵のカプセル化) および ML-DSA (FIPS 204 デジタル署名)
- ステートフルなハッシュベースの署名: LMS および マルチレベルHSS (RFC 8554 / NIST SP 800-208)

楕円曲線暗号(ECC)

- ECDSA/ECDH および ECIES 用の FIPS 承認済み NIST プライム曲線 (P-192、P-224、P-256、P-384、P-521) および Brainpool 曲線 (P192~P512)
- BIP32 階層的決定性ウォレット鍵管理用の Koblitz 曲線 (secp256k1)
- Montgomery 曲線 (X25519、X448) および Edwards 曲線 (Ed25519、Ed448)

非対称および対称

- 非対称: RSA (最大4096ビット鍵サイズ)、標準PKCS#1 v1.5、OAEP、および FIPS 承認済み PSS 確率的署名生成に対応
- 対称: AES (128、192、256ビット)、ECB、CBC、CBCPAD、CTR、GCM、GMAC、Key Wrap、および 512ビット AES-XTS モードに対応 ARIA、SEED
- レガシー: 後方互換性のあるアンラッピング/復号化専用に保持された Triple-DES (3DES) CBC/ECB

セキュアハッシュ、KDF、および通信

- SHA-2 および SHA-3 セキュアハッシュ (224~512ビット) および HMAC
- SHAKE-128、SHAKE-256 拡張出力関数 (XOF)
- 鍵導出: NIST SP 800-108 カウンターモード
- 鍵ラッピング: NIST SP 800-38F
- 3GPP モバイル通信セルラーセキュリティ: MILENAGE、TUAK、および COMP128 加入者認証プロファイル

デジタルウォレットおよびブロックチェーンカストディ

- BIP32 および SLIP10 階層的決定性 (HD) 鍵管理

乱数生成

- NIST 800-90A 準拠の HMAC_DRBG とともに HW ベースの真性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

セキュリティ認定

- FIPS 140-3 Level 3*
- 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 2 規則 準拠の適格電子署名生成装置 (QSCD) の リストに掲載*

ネットワーク

- マルチモードまたはシングルモード光ファイバーおよび RJ45 銅線対応の 10G SFP+ (x 4)
- IPv4、IPv6*、ポートボンディング*
- ベースボード管理コントローラー (BMC) 用 1G RJ45 イーサネットポート (x 1)

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:
 - 17.44" (幅) x 21.95" (奥行) x 1.71" (高さ)
 - 443mm (幅) x 557.6mm (奥行) x 43.5mm (高さ)
- 重量:
 - シングルモジュールアプライアンス 26.5lbs (12kg)
 - デュアルモジュールアプライアンス 30lbs (13.6kg)
- 入力電圧: 100~240VAC、50-60Hz
- 標準消費電力:
 - シングルモジュールアプライアンス 約 135W
 - デュアルモジュールアプライアンス 約 270W
- 最大消費電力:
 - シングルモジュールアプライアンス 約 225W
 - デュアルモジュールアプライアンス 約 450W
- 温度: 動作時 0°C~40°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

- 80 PLUS Platinum 認証取得
- UL, CSA, CE
- FCC, CE
- RoHS3, 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およびファン
- 平均故障間隔 (MTBF)
 - シングルモジュールアプライアンス: 289,444 時間
 - デュアルモジュールアプライアンス: 171,236 時間

管理および監視

- 量子安全 HA フェイルオーバー/負荷分散
- 量子安全ハードウェア間バックアップと復元
- アウトオブバンド診断用 rsyslog および BMC



利用可能なLuna Network HSMモデル

モデル			
	Luna 100 (標準パフォーマンス)	Luna 150 (エンタープライズパフォーマンス)	Luna 190 (最大パフォーマンス)
コンテナ数	1	最大6	最大15
鍵ストレージ	128 MB	1024 MB	4096 MB

Luna 8 Network HSMは、性能、鍵容量、サポートされるコンテナ数に基づき、3つのモデルで提供されます。各モデルは一般的な導入要件に合わせて設計されているため、お客様の環境に適したソリューションが簡単に選べます。各セキュアコンテナは、分離されたLuna 8 HSMインスタンスをホストし、最大10のパーティションをサポートします。

タレスについて

タレスはデータセキュリティのグローバルリーダーとして、世界中で高い信頼を得ているさまざまな組織が、あらゆる場所で重要なアプリケーション、機密データ、およびIDを包括的に、かつ最高の投資対効果(ROI)で保護できるよう支援しています。フォーチュン・グローバル500企業の58%を含む3万社以上の顧客を抱え、そのソリューションは世界148カ国で導入されています。タレスは、革新的なサービスと統合プラットフォームを通じて、リスクの可視化、サイバー攻撃の防御、そしてコンプライアンスギャップの解消を可能にし、毎日数十億人の消費者に安心して信頼性の高いデジタルエクスペリエンスを提供します。