

Data sheet

Luna USB HSM

cpl.thalesgroup.com

THALES
Building a future we can all trust

Luna USB HSMは、小型フォームファクタのHSMです。データ、アプリケーション、デジタルIDを保護してリスクを低減し規制コンプライアンスを確保するために、政府機関、金融機関、大企業によって広く使用されています。Luna USB HSMは、PKIルート鍵の強力な保護に最適です。

- ポータブルなハンドヘルドの小型フォームファクタデバイス
- 容易なセットアップ – 数分で稼働
- LCDタッチスクリーンにより、ファームウェア、メモリ容量などのステータスを素早く確認可能
- ホスト電源USB – 外部電源アダプタが不要
- コーラム (MofN) 多要素認証のスタンドアロンサポートにより、セキュリティを強化

Luna USB HSMの概要

Luna USB HSMは、耐タンパ性を備えたハードウェア内にすべての暗号化された鍵マテリアルを保存することにより、高保証の鍵保護を提供します。小型フォームファクタとオフラインの鍵ストレージ機能が、本製品の特徴です。ビジネスクリティカルな鍵をセキュアなオフライン環境で保護する必要がある場合に最適です。

共通のアーキテクチャ

Luna HSMは、Luna Network、Luna PCIe、Luna Cloud HSMを含む製品ライン全体で共通のアーキテクチャを備えており、クライアント、API、アルゴリズム、認証方式が一貫しています。このため、特定のHSMを中心にアプリケーションを設計する必要がなく、ビジネスニーズの変化に応じて、HSMからHSMへ、オンプレミスからパブリッククラウドやプライベートクラウドへ、鍵を柔軟にクローニングできます。

メリットと特徴

高保証のセキュリティ

- FIPS 140-3検証済み*の侵入に強いハードウェアに、鍵を常に保管
- 迅速なディザスタリカバリのためのリモート管理、バックアップ、復元
- パスワード認証またはコーラム (MofN) 多要素認証による、セキュリティの強化と強力な職務分掌
- セキュアな転送モードによる高保証の配信を実現



使用例

- PKI鍵の生成と鍵の保管/保護 (オンラインCA鍵とオフラインCA鍵)
- 証明書の検証と署名
- オフラインのハードウェア保護/ビジネスクリティカルな鍵のセキュリティ
- BYOK (独自の鍵の持ち込み) のユースケースのサポート

暗号の俊敏性

Luna USB HSMは、幅広い非対称鍵暗号化と鍵交換機能に加え、標準対称鍵暗号化アルゴリズムもすべてサポートしています。また、すべての標準ハッシュアルゴリズムとメッセージ認証コード (MAC) もサポートしています。Luna USB HSMには、NIST SP 800-90AおよびBに準拠したハードウェアベースの乱数発生器が搭載されています。

パフォーマンス

オペレーション	鍵	TPS
署名	RSA-1024	340
署名	RSA-2048	62
署名	RSA-4096	8
署名	ECC P256	48
署名	ECC P521	8
暗号化	ECIES (AES128-SHA256 HMAC P256)	24
暗号化	AES256-GCM	1350

技術仕様

Luna USB HSM U700

- 1パーティション、32MB

OSサポート

- Windows, Linux

クライアント

- Thales Luna Universal Client

暗号化APIサポート

- PKCS#11, Java (JCA/JCE)、Microsoft CAPIおよびCNG、OpenSSL

暗号化

- Suite Bの完全サポート
- 非対称: RSA、DSA、Diffie-Hellman、楕円曲線暗号 (ECDSA、ECDH、Ed25519、ECIES)、KCDSAなど
- 対称: AES、AES-GCM、Triple DES、DES、ARIA、

SEED、RCS、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およびB Hash-DRBGとともにハードウェアエントロピー源を使用
- デジタルウォレット暗号化: BIP32

セキュリティ認定

- FIPS 140-3 Level 3

物理的特徴

- 寸法: 6.3" x 3.43" x 1.03" (160.02mm x 87.12mm x 26.16mm)
- 重量: 0.9lb (410g)
- 4.7" LCDタッチスクリーン
- 温度: 動作時 0°C~40°C、保管時 -20°C~70°C
- 相対湿度: 20%~95% (38°C) 非結露
- 消費電力: 最大7.2W、標準4.5W
- 外部USB AC: 入力電圧: 100~240V、50~60Hz / 出力 5VDC 3A
- ホストインターフェース: USB 3.0 Type Cコネクタ
- トークンインターフェース: USB 3.0 Type Cコネクタ + USB-C(メス)to USB-A(オス)変換アダプタ

安全・環境コンプライアンス

- UL, CSA, CE
- FCC、KCマーク、VCCI、CE
- RoHS, WEEE
- India BIS [IS 13252 (Part 1)/IEC 60950-1]

信頼性

- MTBF: 560073 hrs@40C, Telcordia SR-332, Issue C

貿易協定コンプライアンス

- TAA