wisecuretech

VeloCrypt® MicroSD HSM

世界最小サイズ
同クラス最高速のHSM

暗号システムにおける最も重要な「鍵（キー）」は、安全な環境で保管され暗号演算を行う必要があります。「ハードウェアセキュリティモジュール（HSM）」は、システムセキュリティの信頼の根幹（Root of Trust）として、世界中の重要インフラ、軍事・行政機関、金融機関において不可欠な存在です。しかし従来の HSM は拡張カード型が主流であり、モバイル端末やエンドポイントデバイスでは直接利用できません。

VeloCrypt MicroSD は、世界最小クラスの HSM として、モバイルやエンドポイントにおける高度なセキュリティ要求に対応。高速なデータ暗号化保存、鍵の生成と管理、デジタル署名、認証などの暗号機能を提供し、安全な認証、起動、機密データ保護、安全通信を実現します。新たな応用領域における高まる安全ニーズに応え、正しいセキュリティ基盤のもと、安定した業務運用を支援します。

物理セキュリティ

CC EAL5+ 認証のセキュリティチップと精密な内部回路設計により、サイドチャネル攻撃などのハードウェア攻撃を防ぎ、軍用レベルの高度な鍵保護対策を実現します。

システムセキュリティ

セキュリティ重視のファームウェア設計を採用し、機密データや鍵が静的に保存されている場合も、動的に転送される場合も、システム全体で保護します。

静的データ暗号化

512MB～32GB の暗号化領域を確保し、強力な認証機構でアクセスを制御。保存データの暗号化を実現します。

インターフェース互換性

SDIO インターフェースとシンプルなサービスアクセス設計により、各種組込みシステムやデバイスに幅広く対応。ハード・ソフト両面の開発負担を軽減し、製品の開発期間とコストを削減。市場投入を加速します。

暗号サービスと性能

各種標準暗号アルゴリズムを内蔵し、幅広いセキュリティニーズに対応。AES 暗号化ストレージは最大 10MB/s の高性能を実現し、高い安全性と処理能力で強固な防御環境を構築します。

ワイセキュア株式会社　WiSECURE Inc.

〒105-6490 東京都港区虎ノ門1丁目17-1 虎ノ門ヒルズ ビジネスタワーCIC Tokyo, 15F
連絡担当：Rose Lin（日本語対応可）　048-400-3057　rose@wisecure-tech.jp

https://wisecure-tech.jp

Secure Boot

VeloCrypt SA シリーズは、デバイスにハードウェアレベルの信頼の基点（RoT）を提供し、改ざん防止機構と高度な認証により、鍵の安全を確保。起動時にはシステムの整合性を検証し、信頼されたファームウェアと OS のみを実行させることで、マルウェアの侵入やネットワーク乗っ取りを防止。起動から稼働まで、常に信頼された環境を維持します。

FIDO Device OnBoard (FDO)

VeloCrypt SA シリーズは、kvFDO サービスと組み合わせることで、既存の IoT 機器に搭載可能。FDO 標準プロトコルを通じて、企業の SaaS 型デバイス管理システムに接続し、自動化された迅速な機器展開を実現。運用効率とライフサイクル管理の透明性を大きく向上させます。

機密データの暗号化と保存

VeloCrypt SA シリーズは、高速な暗号化ストレージ性能とセキュリティチップによる軍用レベルの保護を両立。柔軟に設定可能な暗号化領域により、さまざまな用途で高いセキュリティとスムーズな処理性能を維持し、デバイスのデジタル資産を守ります。

エンドツーエンドのセキュア通信

VeloCrypt SA シリーズは、ハードウェアベースの保護に加え、ソフトウェア開発キット（SDK）を提供。メーカーは既存アプリとの統合が可能で、複数の通信プロトコル間におけるデータ転送の安全性を確保。盗聴や改ざんへの耐性を強化します。

製品仕様 VeloCrypt SA Series

外形サイズ：SD メモリーカード形式
フラッシュタイプ：SLC / MLC
ストレージ容量：512MB / 8GB / 16GB / 32GB
動作温度範囲：0℃ ～ 70℃ | 保存温度範囲：-40℃ ～ 125℃
動作電圧：2.7V ～ 3.6V
消費電流：160mA + 35mA

ハードウェア特長

- SD Default Speed / SD High Speed / SD UHS-I に対応
- CC EAL5+ 認証取得の高セキュリティチップ採用
- CE / FCC / VCCI / BSMI 各種安全規格に準拠
- PKCS#11 / ネイティブ API 対応

暗号アルゴリズム対応一覧

- メッセージダイジェスト：SHA-2 / SHA-3 / HMAC
- 公開鍵暗号：RSA 2048bit
- 楕円曲線暗号（ECC）：
- 素数域カーブ（最大 521bit）
- エドワーズ曲線対応
- 対応プロトコル：ECDSA / ECDH
- 対称鍵暗号（AES）：ECB / CBC モード対応
- 乱数生成：
  AIS-31（PTG.2）認定ハードウェア TRNG
  NIST SP800-90A 準拠の Hash-DRBG