Wisecure Technologies

MICRO HSM

— µSD/X

Features 製品の特長

Use cases 運用例の紹介

Security and crytographic features セキュリティと暗号化機能

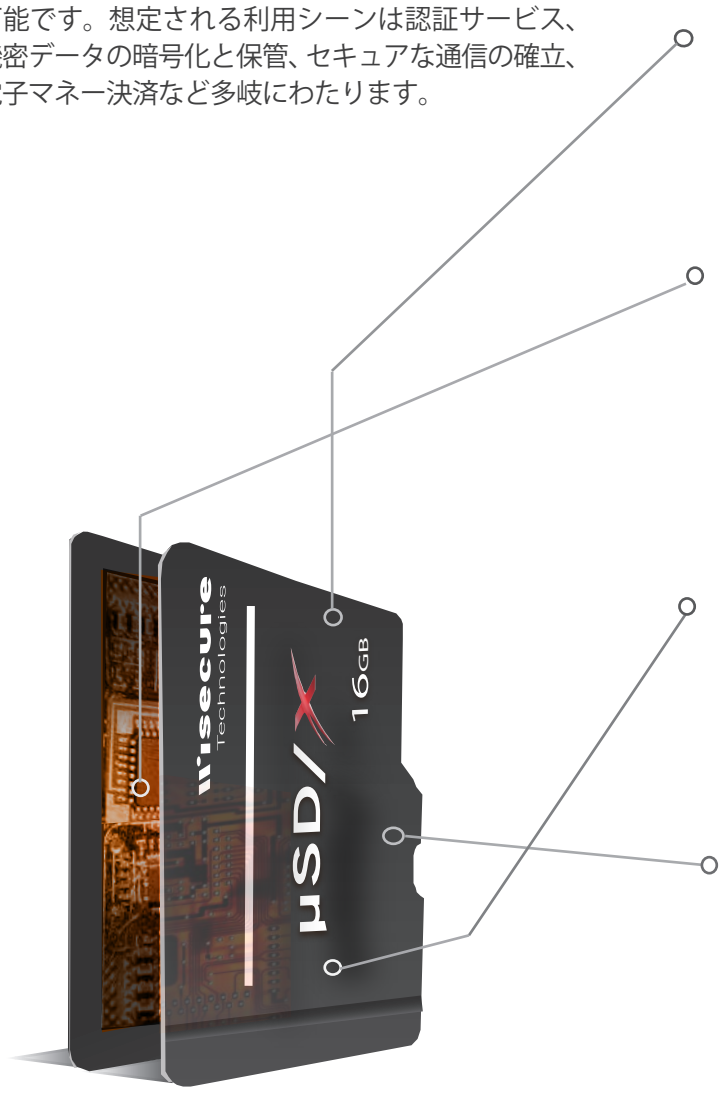
Hardware specification ハードウェア仕様

世界最小サイズ、最速の HSM

“

暗号化システムの鍵となる「暗号キー」は、最も安全な環境で保管と暗号化演算を行う必要があります。そのため、ハードウェア・セキュリティ・モジュール (HSM) で物理的にセキュリティを確保し管理することが一般的です。その一方、それはサーバー側での使用に限定され、エンドポイントデバイスの安全性は担保されていません。

この問題点を解決できるµSD/X は、HSM の高い安全性と全ての機能を持つ以外に、MicroSD カードの利点も備えており、エンドポイントデバイスでの暗号化を安易に実現可能です。例えば、暗号化 / 復号化処理、暗号鍵の作成とライフサイクルの管理、デジタル署名と認証サービスなどが含まれます。弊社独自の設計により、µSD/X の性能は他社製品よりはるかに優れ、7MB/ 秒もの高速なデータ暗号化処理が可能です。想定される利用シーンは認証サービス、機密データの暗号化と保管、セキュアな通信の確立、電子マネー決済など多岐にわたります。



製品の特長

インタフェースの互換性

互換性の高い SDIO インタフェースにより、既に導入済みのマシンにも容易に導入が可能です。また、互換性が高いため、セキュリティシステムを導入する際の時間を短縮でき、製品やサービスの開発速度を加速させます。

物理的セキュリティ

CCEAL 5+ 認定を取得したその軍事レベルに堅牢な内部回路設計は、近年増加するサイドチャネル攻撃 (SCA) などの物理的手段によるサイバーアタックからも暗号キーを守ることをお約束します。

システムセキュリティ

高度なセキュリティレベルが設定されたファームウェア・アーキテクチャにより、システム動作中及び休止中の機密データに対して安全な環境をご提供します。

パフォーマンスに優れた暗号化サービス

本製品は複数の対称/非対称アルゴリズム対応APIをご提供しています。その内のひとつであるAESでは7MB/秒での暗号化処理を実現しています。その他、複数の暗号通貨取引にも採用されているより安全なEdDSA(エドワーズ曲線デジタル署名アルゴリズム)等の様々な暗号化アルゴリズムがご利用可能です。

運用例の紹介

IoT 等のネットワーク認証システムでの活用

µSD/X 用に構築されたソリューションは無線（OTA）によるファームウェアのアップデート、パラメーター更新、デバイス管理など様々なシーンで活躍します。パブリックキー（公開鍵）の証明書発行やプライベートキー（秘密鍵）の検証による暗号化サービスを提供することで、データの改ざんやデバイスの乗っ取りなどのセキュリティリスクを排除することができます。

機密情報の暗号化と保存

µSD/X は柔軟にパーティションを割り当てることが可能なため、暗号化された記憶領域（セクター）とそうでない領域に割り当てることができ、認証取得済のユーザーだけが暗号化された領域にアクセスできます。カスタマイズ可能なハードウェア暗号エンジンを採用し、ハイパフォーマンスでセキュアな暗号化・復号化の処理を提供し、通信状態のオンライン/オフラインに関係なくデータへのセキュアなアクセスや保存を確保します。一般的なソフトウェアベースのサービスや製品は、ハッキングに対しての根本的な防御能力はありません。その一方、セキュリティチップで実現されたライバル社製品の場合、スムーズなデータ操作性能を満たすことができません。**µSD/X** はハイスピードな暗号化処理とセキュリティチップによる高い堅牢性を両立させ、ユーザーはパフォーマンスに妥協せずに完璧なハードウェア・セキュリティを確保できます。

安全なデバイス間通信（P2P通信）の実現

µSD/X は例えば Telegram や Signal といった個人間メッセージ通信での、高速なデータ暗号化といったニーズに対しても柔軟に対応可能です。潜在的な脆弱性が組み込まれる恐れのあるソフトウェアベースの暗号化通信に比べ、ハードウェアベースの µSD/X は盗聴や改ざんといったリスクに対する抵抗力を高めます。また Signal やその他のアプリケーションに対して、ユーザフレンドリーな暗号化ソリューションを提供する為のソフトウェア開発キット(SDK）がご用意されています。高い互換性を実現すると共に、ハイレベルな安全性をも併せ持つ µSD/ X のソリューションは、どのプラットフォームとデバイスに対しても迅速な導入が可能な為、時間と運用コストを大幅に削減できます。

暗号通貨取引の安全対策

µSD/X は暗号通貨用プライベートキー (秘密鍵) の保存と取引時のデジタル署名機能をサポートします。モバイル端末に紐づくことで、メモリカードリーダーや USB トークン等の他のデバイス無しにあなたのモバイル端末をハードウェアウォレット (コールドウォレット) として使用することが可能になります。CC EAL 5+ 認証取得済の最高レベルのセキュリティチップを用いた安全性により、秘密鍵の漏えいを防ぎ、サイドチャネル攻撃や悪意あるリバースエンジニアリング対策にも効力を発揮します。

セキュリティと暗号化機能

サポートする暗号化アルゴリズム

メッセージダイジェスト：SHA-2、SHA-3、HMAC、RSA 2048/4096
ECC（楕円曲線暗号:最大521bit）※エドーワード曲線を含む
ECCプロトコル：ECDSA、ECIES、ECDH、EdDSA(FIPS186-5)
AES256モード：ECB、CBC、CFB、OFB、GCM、XTS
乱数発生器：AIS-31（class　PTG2）※Hash_DRBG in NIST SP800-90Aに準拠
ECC及びAES向けのカスタマイズ可能な暗号化エンジン

アプリケーションプロトコル

暗号通貨：BIP32、BIP39、BIP44
認証方式：Fido U2F

API

PKCS#11
Android Keystoreプロバイダ
ネイティブAPI

ハードウェア仕様

インタフェース

SD3.0（UHS-I）およびSD2.0完全準拠

本体サイズ規格

microSD

フラッシュメモリ容量

16GB（最大32GB）

消費電力

動作モード：160mA
待機モード：85～90mA
スリープモード：20～25mA

温度

保存温度：-40°C ~ 125°C
動作温度：0 °C~ 70°C

柔軟なカスタマイズ性と
スピーディな開発環境のご提供

“

μSD/X はその柔軟なハードウェア構造設計により、標準的なアルゴリズムはもちろんのこと、様々なアルゴリズムでのシステム開発とカスタマイズが可能です。現在稼働中のシステムにそのまま導入することが可能で、既存のハードウェアに対しての追加・更新を必要としません。またお客様が独自の非対称曲線アルゴリズムや、ハードウェア暗号化エンジン、μSD/X 用ハードウェアアクセラレータ等を必要とされる場合には、私達はその実現や構築のお手伝いをするための専門的なサポートサービスをご提供いたします。

またそう遠くない未来に顕在化する、「量子コンピューター」がもたらす脅威への対抗策のために、私たちは「耐量子コンピュータ暗号 (PQC)」の開発に専念し、その最先端技術をμSD/X を始めとする自社製品に組み込むことでお客様の長期的な情報セキュリティに対するニーズに応えていきたいと考えています。

WiSECURE は第四次産業革命の新時代おいて求められる、お客様のデリケートで大切なデジタル資産の保全ニーズにフォーカスし、弊社の得意とするハードウェアセキュリティモジュール（HSM）を通じて、サイバー攻撃等の悪意ある攻撃からのリスクから遠ざけます。

wisecure Technologies