



ENTRUST

nShield Edge HSM

デスクトップアプリケーションに暗号鍵サービスを提供する、
認定取得済みUSB接続型デバイス

ハイライト

nShield Edgeハードウェア・セキュリティ・モジュール (HSM) は、FIPS認定を受けた完全装備のUSB接続型デバイスで、利便性と経済性に加え、暗号化と鍵の生成および保護機能を提供します。

- コスト効率を最大化する、nShieldシリーズの中で最も経済的なHSM
- 認証局やコードサイニングなどさまざまなアプリケーションをサポート
- FIPS 140-2レベル3までの認定を取得し、強力なセキュリティを提供

少量の取引を処理する環境向けの設計

オフラインでの鍵生成や開発環境に適しており、アルゴリズムとAPIも完全にサポートします。クラウドに暗号鍵を安全にエクスポートする前に、FIPS 140-2レベルの保証のもと、暗号鍵の生成を必要とする独自の鍵の持ち込み (BYOK) を展開するのに最適です。

優れた可搬性

便利なUSBインターフェイスを備えた小型・軽量設計により、ラップトップやその他のポータブルデバイスを含むさまざまなプラットフォームをサポートします。

高い費用対効果と拡張性

nShieldシリーズの中で最も経済的なnShield Edgeは、エントリーポイントとしてのHSMとして機能すると同時に、ニーズの拡大に応じて環境を拡張することができます。Entrust独自のSecurity Worldアーキテクチャにより、nShield HSMを組み合わせ、柔軟な拡張性、鍵の共有、シームレスなフェイルオーバー、負荷分散を実現する複合システムを構築することができます。



nShield Edge HSM

技術仕様

サポート対象の暗号化アルゴリズム (完全なNIST Suite Bの実装を含む)	オペレーティングシステム	アプリケーションプログラミングインターフェイス (API)	互換性とアップグレード可能性	セキュリティ関連のコンプライアンス
<ul style="list-style-type: none">非対称アルゴリズム: RSA、Diffie-Hellman、ECMQV、DSA、El-Gamal、KCDSA、ECDSA、ECDH、Edwards (X25519、Ed25519ph)対称アルゴリズム: AES、Arcfour、ARIA、Camellia、CAST、DES、Triple DES、MD5 HMAC、RIPEMD160 HMAC、SEED、SHA-1 HMAC、SHA-224 HMAC、SHA-256 HMAC、SHA-384 HMAC、SHA-512 HMAC、Tiger HMACハッシュ/メッセージダイジェスト: MD5、SHA-1、SHA-2 (224、256、384、512ビット)、HAS-160、RIPEMD160	<ul style="list-style-type: none">Microsoft Windows 7 x64、10 x64、Windows Server、2012 R2 x64、2016 x64、および2019 x64Red Hat Enterprise Linux AS/ES 6 x64、x86、7 x64、および8 x64、SUSE Enterprise Linux 11 x64 SP2、12 x64、および15.1 x64Oracle Enterprise Linux 6.10 x64、7.6 x64、および8 x64	<ul style="list-style-type: none">PKCS#11、penSSL、Java (JCE)、Microsoft CAPI およびCNG、nCore、Webサービス (nShield Web Services Option Packが必要)	<ul style="list-style-type: none">USBポート (1.x、および 2.x 準拠)	<ul style="list-style-type: none">FIPS 140-2 レベル2およびレベル3、NIST SP 800-131A

安全基準および環境基準への準拠	管理およびモニタリング機能	物理的特性	性能
<ul style="list-style-type: none">UL、CE、FCC、現カタログはC-TICK カナダのICES RoHS2、WEEE	<ul style="list-style-type: none">安全な監査ログ取得Syslog診断サポートおよびWindowsパフォーマンスモニタリングSNMPモニタリングエージェント	<ul style="list-style-type: none">スマートカードリーダー内蔵のポータブルデスクトップ型デバイススタンドを開いた状態の寸法: 120 x 118 x 27mm (4.7 x 4.6 x 1インチ)重量: 340g (0.8ポンド)入力電圧: 5V DC (USBホストデバイスより)消費電力: 700mW	<p>NIST推奨の鍵長での署名パフォーマンス:</p> <ul style="list-style-type: none">2048ビットRSA: 2tps4096ビットRSA: 0.2tps

利用可能なモデルと性能

- nShield Edge FIPS レベル2、および nShield Edge FIPSレベル3
- 非FIPSの開発者版 nShield Edgeも提供

詳細

Entrust nShield HSMの詳細については、entrust.com/ja/HSMをご覧ください。アイデンティティ、アクセス、通信、データ向けのEntrustのデジタルセキュリティソリューションの詳細については、entrust.com/jaをご覧ください。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

