Entrust nShield® 5s HSM

暗号化キー サービスをスタンドアロン サーバーに提供する認定 PCI Express カード

特長

Entrust nShield® 5s ハードウェア セキュリティ モジュール (HSM) は、サーバーまたはアプライアンスでホストされているアプリケーションに暗号化サービスを提供する、FIPS 140-3 (評価中の認証) のロープロファイル PCI Express カードです。認証局、コード署名、カスタム ソフトウェアなどを含む広範なアプリケーションで、暗号化、デジタル署名、あん号鍵生成などの機能を実行します。

柔軟性の高いアーキテクチャ

nShield 5s は、Entrust 独自の Security World アーキテクチャにシームレスに適合する HSM の最新製品です。Security World を使用すると、複数の nShield HSM を組み合わせて、柔軟な拡張性、シームレスなフェイルオーバーと負荷分散を実現する混合資産を構築できます。

高い処理能力

nShield 5s HSM は高いトランザクション レートをサポートしており、スループットが重要なエンタープライズ、小売、IoT、その他の環境に最適です。

シンプルな監視と一元管理

Security World ソフトウェアで利用できる新しい GUIベースの KeySafe 5 により、組織は HSM および関連する Security World の資産をリモートで効果的に監視し、一元管理できます。

強力なリモート管理

nShield 5s リモート管理オプション - 新しい HSM の登録や既存の HSM の再割り当て/再構成などのメンテナンス タスクを実行するために、リモート HSM への認証スマート カードの安全なリモート プレゼンテーションを有効にします。

主な機能と利点

- 高い暗号化トランザクションレートと柔軟なスケーリングにより、パフォーマンスと可用性を最大化します
- 認証局、コード署名などを含むさまざまなアプリケーションをサポート
- FIPS 140-3 認証 (評価中)
- nShield リモート管理オプションはコストの削減と出張費の削減に役立ちます

より詳細については、entrust.com/ja/HSMをご覧ください。

nShield 5s HSM

技術仕様

サポートする暗号アルゴリズム

- NIST Suite B の完全実装
- 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, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, 3DES
- ハッシュ/メッセージダイジェスト: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160, SHA-3 (224, 256, 384, 512 bit)
- 楕円曲線鍵協定 (ECKA) は Java API および nCore API 経由で利用可能 楕円曲線統合暗号化スキーム (ECIES) は Java API、PKCS#11 および nCore API 経由で利用可能
- TUAK アルゴリズムによる相互認証およびキー生成のサポート (3GPP)

サポートするプラットフォーム

- 仮想マシンまたはコンテナ内で実行される RedHat、SUSE、および主要なクラウド サービス プロバイダーのディストリビューションを含む Windows および Linux オペレーティング システム

サポートするAPI

- PKCS#11、OpenSSL、Java (JCE)、Microsoft CAPI および CNG、nCore、および Web サービス (nShield Web サービス オプション パックが必要)

ホスト接続性

- PCI Express バージョン 2.0; コネクタ: 4レーン

セキュリティコンプライアンス

- FIPS 140-3 レベル 3 評価中
- nShield 5s: BSI AIS 20/31 準拠

安全および環境基準の遵守

- UL, UL/CA, CE, FCC, Canada ICES, KC, FCC, VCCI, RCM, UKCA
- RoHS2, WEEE, REACH

管理と監視

- nShield リモート管理と nShield モニター
- 安全な監査ログ
- Syslog診断サポートとWindowsパフォーマンス監視
- SNMP監視エージェント

対応機種と性能

nShield 5s モデル	ベース	ミドル	ハイエンド
NIST 推奨の鍵長の RSA 署名パフォーマンス (tps)			
2048 ビット			
4096 ビット			
NIST 推奨の鍵長の ECC プライム曲線署名パフォーマンス (tps)			
256 ビット			
ECC アクティベーションによるキー生成 (キー/秒)			
RSA 2048 ビット			
ECDSA P-192 ビット			
ECDSA P-256 ビット			
ECDSA P-521 ビット			

詳しくはこちらは:
entrust.com/ja

ENTRUST

エントラストジャパン株式会社
DPS事業本部
東京都港区台場二丁目3番1号
トレードピアお台場
HSMinfo@entrust.com