Entrust nShield® 5c HSM

アプリケーションのセキュリティは、鍵をどこに保管するかによって決まります

特長

総合力

Entrust nShield® 5c ハードウェア セキュリティ モジュール (HSM) は、ネットワーク全体にスケーラブルで可用性の高い暗号キー サービスを提供する FIPS 140-3 レベル 3 (評価中) アプライアンスです。

- 高い暗号化トランザクション率と柔軟なスケーリング
- 150 を超える主要なアプリケーション プロバイダー ソリューションと統合
- 簡単なインストールによる強力なリモート構成および管理機能

nShield 5c HSM は、暗号化、デジタル署名、キー生成などの機能を実行し、次のようなさまざまなアプリケーションやテクノロジーをサポートする耐タンパー性のアプライアンスです。

- 認証局
- コード署名
- カスタムソフトウェア
- クラウドおよびコンテナ化されたアプリケーション
- ウェブサービス
- リモート署名
- ブロックチェーン
- データベースの暗号化
- 5G/IoTアプリケーション

より詳細については、entrust.com/ja/HSMをご覧ください。

nShield 5c HSM

主な機能と利点

柔軟性の高いアーキテクチャ

nShield 5 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。Entrust Security World を使用すると、nShield HSM モデルを組み合わせて、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 5c HSM は高いトランザクション レートをサポートしており、5G、Car2X、IoT などのスループットが重要なアプリケーション環境に最適です。

シンプルな一元管理

KeySafe 5 - Security World ソフトウェアを使用すると、組織は HSM および関連する Security World の資産をリモートで一元管理できます。

強力な nShield 5 リモート オプション

データセンターへの訪問が不要に

nShield リモート管理 - 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。 別途データシートをご用意しております。

リモート設定 - シリアル コンソールを使用すると、データ センターのスタッフが簡単にインストールでき、HSM のフロント パネルやフロント パネルの設定に物理的にアクセスする必要なく、HSM とクライアントの構成が可能になります。

nShield モニター - すべての nShield HSM の単一のダッシュボードを提供し、運用の最適化と稼働時間の増加に役立ちます。

対応機種と性能

nShield 5c 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	670	3,949	13,614
4096 ビット	135	814	2,200
8192 ビット	19	115	309
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	2,085	7,553	21,826
521 ビット	1010	5,977	16,164
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	7	20	23
ECDSA P-256 ビット	1,040	3,580	3,494
ECDSA P-521 ビット	518	2,480	2,724
主要な合意のパフォーマンス (トランザクション/)			
ECDH P-256 ビット	2,085	7,550	21,436
クライアントライセンス数			
標準で含まれている数	3	3	3
最大	10	20	無制限 [1]

注 1: エンタープライズ クライアント ライセンスが必要です。

nShield 5c 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 (including NIST, Brainpool & secp256k1 curves), ECDH, Edwards (Ed25519, Ed25519ph
- 対称アルゴリズム: AES, AES-GCM, 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)
- Java API および nCore API 経由で利用可能な楕円曲線鍵協定 (ECKA)
- Java API、PKCS#11、および nCore API 経由で利用可能な楕円曲線統合暗号化スキーム (ECIES)
- 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/CNG
- Web サービス (Web サービス オプション パックが必要)
- nCore

ホスト接続性

- デュアル ギガビット イーサネット ポート (ネットワーク ボンディング オプションを備えた 2 つのネットワーク セグメント)

セキュリティコンプライアンス

- FIPS 140-3 レベル 3 評価中
- IPv6認定およびUSGv6 Ready準拠
- BSI AIS 20/31 準拠

安全および環境基準の遵守

- UL, CE, FCC, UKCA, RCM, Canada ICES, RoHS, WEEE, REACH

高可用性

- すべてのソリッドステートストレージ
- フィールドサービス可能なファントレイ
- デュアルホットスワップ電源装置
- HSM のクラスタリングと自動フェイルオーバー/ロード バランシングの完全なサポート
- アクティブバックアップモードと802.3adモードをサポートするネットワークボンディング

管理と監視

- nShield リモート構成
- nShield リモート管理 (別途購入)
- nShield モニター (別途購入)
- 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

物理的特徴

- 標準1U 19インチ。ラックマウント寸法: 43.4 x 430 x 705mm
- 重量: 11.5kg
- 入力電圧: 100-240V AC 自動切り替え 50-60Hz
- 消費電力: 110V AC、60Hz で最大 2.0A | 1.0A (AC220V、50Hz)
- 熱放散: 327.6 ～ 362.0 BTU/時 (全負荷)
- 信頼性 - MTBF (時間)[2]: 107,845 時間

注2：Telcordia SR-332「電子機器の信頼性予測手順」MTBF規格を使用し、動作温度25℃で計算

お問合せはこちら

03-4221-9718

HSMinfo@entrust.com

entrust.com/ja/HSM

ENTRUST CORPORATIONについて

Entrustは、信頼できる認証、支払い、データ保護を実現することで、動き続ける世界をセキュアにしています。今日、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザー体験が求められています。Entrustは、これらの要となる部分において、他に類を見ない幅広いデジタルセキュリティとID発行ソリューションを提供しています。2500人を超える従業員、グローバルパートナーネットワーク、そして10カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

詳しくはこちらは：
entrust.com/ja

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