High-scalability Keystore (HSK)

高性能で同時に数百万の鍵を処理

ハイライト

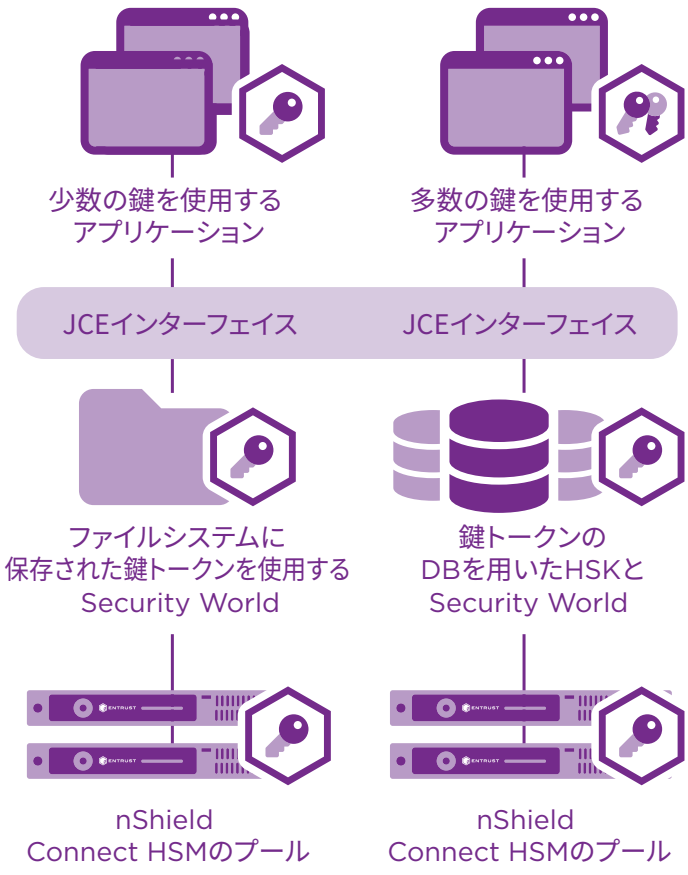
- 特定のEntrust nShield® HSMユースケース向けの高性能、でスケーラビリティの高いソリューション
- 大量のアクティブ暗号鍵を同時に処理可能
- OSのボトルネックを回避

一部のハードウェア・セキュリティ・モジュール（HSM）では、非常に多数の暗号鍵を同時に処理することが必要になる場合があり、HSMに接続しているコンピュータのファイルシステムにもボトルネックが発生する可能性があります。High-scalability Keystore（HSK）は、大量の鍵を高性能でサポートします。

鍵の特長

HSKソリューションは次の機能を提供します。

- 数百万のRSA鍵に拡張可能
- 鍵の数が増えても、パフォーマンスは基本的に一定
- RSA鍵の生成、証明書署名要求（CSR）の生成、デジタル署名の作成と検証、データの暗号化と復号化をサポート
- 複数の呼び出し元のコンピュータ間の自動同期
- ニーズに合わせてカスタマイズできる拡張可能なソリューション



詳細をチェック：ENTRUST.COM/ja/HSM

High-scalability Keystore (HSK)

しくみ

Entrust nShield HSMは、1秒あたり数千のトランザクションをサポートする高性能のトランザクションスループットを提供します（パフォーマンスは、HSMモデルと特定の暗号化操作によって異なります。最新のHSMの性能詳細については、各nShieldモデルのデータシートをご参照ください）。

Entrustの柔軟で安全なSecurity Worldアーキテクチャは、HSMの外部にある暗号鍵を「トークン」として保存します。「トークン」内の鍵は、暗号化、使用制限、アクセス制御、認証セキュリティを使用して、HSMのマスター鍵の下で厳重に保護されています。これは、非常に強力なセキュリティと、拡張性、負荷分散、フェイルオーバー、プール内のHSM数の簡単な拡張または縮小、プールへの、またはプールからのHSMの交換、追加のバックアップデバイスを必要としない鍵トークンの簡単なバックアップの利点を兼ね備えています。

標準のSecurity Worldアーキテクチャは、トークンごとに1つのファイルを使用して、これらの「トークン」を呼び出し元のコンピュータのファイルシステム（同期をサポート）に格納します。このアプローチは、通常、クライアントコンピュータごとにアクティブな鍵の数が限られているほとんどのユースケースに適しています。

特定のユースケースでは、nShield HSMのパフォーマンスは、呼び出し元のコンピュータのOSのファイルシステムに存在するレイテンシーによって制約される可能性があります。HSKは、ファイルシステムではなく、データベースを使用してクライアントコンピュータに鍵トークンを格納することにより、鍵の数が非常に多い場合に高いパフォーマンスを提供します。

Entrust専門サービス（PS）チームは、HSKが組織のニーズに適しているかどうかを評価するのを支援します。PSコンサルタントはまた、必要に応じて特定の要件に合わせてHSKをカスタマイズするなど、HSKの環境への統合を支援する専門の開発者サポートを提供します。

ユースケースの例

- 多数のユーザを抱える企業のEメールセキュリティ
- 企業文書の署名
- 多数の接続デバイスを備えたモノのインターネット（IoT）
- 多数のエンドユーザを持つモバイルアプリ
- 暗号資産交換のためのeウォレットシステム

技術的情報

- nShield HSMを使用したJava Cryptography Extension（JCE）ライブラリ
- RESTful JSON Web サービスオプション
- nShield HSM鍵の「トークン」をファイルシステムではなくデータベースに保存
- MSSQL、Oracle、Derbyなどの一般的なリレーショナルデータベースソフトウェアで動作（追加のデータベースが追加）
- 負荷分散されたプール内の単一または複数のHSMで動作

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、データに関する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

ENTRUST

お問い合わせ：
HSMinfo@entrust.com