プロダクト ブリーフ

SafeNet ProtectServer Network HSM

SafeNet ProtectServer External 2およびSafeNet ProtectServer External 2+

ジェムアルトのSafeNet ProtectServer Network HSMモデルは、暗号化、署名、および認証サービスをセキュリティ上重要なアプリケーションに提供しながら、暗号鍵を不正アクセスから保護するように設計された、セキュリティを強化したネットワーク暗号化サーバです。

高い安全性

SafeNet ProtectServer Network HSMには、信頼性の高いセキュアな暗号処理を実行する暗号モジュールが含まれています。不正防止のセキュリティが付いた強固なスチールケースにより物理的な攻撃を防ぎ、機密性の高い情報（暗号鍵、PINS、その他データなど）の保管と処理に最高レベルの物理的・論理的保護を提供します。「セキュアな保管と処理」とは、暗号鍵がHardware Security Module（HSM）の外部に使用できる状態でさらされないようにし、他のソフトウェアからは得られないセキュリティレベルを実現することに加え、業界団体のセキュリティ要件を満たす認定レベルの機密性と完全性を提供することを意味します。

柔軟なプログラミング

SafeNet ProtectServer HSMは、アプリケーション開発者が独自のファームウェアを作成してHSMのセキュアな領域内でそれを実行する、他にはないレベルの柔軟性を提供します。機能モジュールと呼ばれるツールキットにより、カスタムファームウェアの開発と導入に必要となる包括的な機能を提供します。柔軟な開発ツール群を完全なものにするフル機能のソフトウェアエミュレータは、開発者にとって便利なデスクトップコンピュータからカスタムファームウェアのテストとデバッグを行えるようにします。このエミュレータは、ProtectServer HSMをインストールせずにアプリケーションをテストする貴重なツールとしても使用できます。準備ができたら、開発者はHSMをインストールして、通信をハードウェアにリダイレクトするだけです。ソフトウェアの変更は必要ありません。

利点

セキュリティ
- 物理的なタンパー保護
- 真性乱数生成
- 鍵マテリアルをスマートカードにバックアップ

パフォーマンス
- デュアルLAN
- 最大1500 RSA署名/秒
- WLD（作業負荷分散）
- マルチスレッドAPI

容易な管理
- インフィールドアップグレード
- GUI HSMインターフェイス
- リモートのHSM管理

拡張APIサポート
- 25、220、1500のパフォーマンスモデルで利用可能なPSE
- 1500パフォーマンスモデルでのみ利用可能なPSE+

容易な管理

直観的なグラフィカルユーザーインターフェイス（GUI）の分かりやすいナビゲーションとユーザー操作により、HSMデバイス管理と鍵管理が簡素化します。緊急のスピードが重視される管理タスク（鍵の変更、追加、削除など）をリモートから安全に実行できるため、管理コストと応答時間が削減されます。

SafeNet ProtectServer PSE2+ HSMは、デュアルスワップ可能なAC電源装置を採用しており、高可用性データセンターを停電から保護できます。また、アプライアンスを2つの別々の電源に接続してソースの一方を誤動作から守ることで、ビジネスの継続性を維持します。これにより装置を確実に動作し続けられるため、故障した電源装置や給電装置のメンテナンスや交換に必要な柔軟性が得られます。

高いパフォーマンスと拡張性

SafeNet ProtectServer Network HSMは、暗号コマンドを迅速に処理します。特殊な暗号電子機器（専用データ暗号マイクロプロセッサ、メモリ、真性乱数生成器（RNG）など）により、暗号処理をホストシステムからオフロードし、より多くの要求に応答できるようになります。

SafeNet ProtectServer Network HSMは、幅広い対称および非対称暗号化パフォーマンスレベルで利用できます。さまざまなセキュリティアプリケーション処理要件に対応し、1秒あたり最大1500のRSA署名処理が可能です。内蔵のデュアルネットワークインターフェイスにより、複数のビジネス領域を保護したり単一のネットワーク内に冗長性を提供したりするために、同じまたは別個のサブネットのいずれかに統合し、異なるネットワーク間で共有できます。また、連携して機能できるHSMの数や管理可能な鍵の数に制限がないため、高いレベルの拡張性・信頼性・冗長性、そしてスループットの向上を容易に実現できます。

利便性

スマートカードは、暗号鍵の安全なバックアップ、リカバリ、転送のための最高のセキュリティと管理上の利便性を提供します。HSMをサービス受付に戻すコストや手間をかけずに、効率よくインフィールドアップグレードを実行できます。

ジェムアルトのSafeNetアイデンティティおよびデータ保護ソリューションについて

ジェムアルトは世界でも最高クラスの完全性を持つエンタープライズセキュリティソリューションを提供しています。本ソリューションにより、お客様はエッジからコアまで、業界をリードするデジタルアイデンティティ、取引、決済、データの保護が受けられます。ジェムアルトが新たに展開するSafeNetアイデンティティおよびデータ保護ソリューションは、重要なデータおよびデータが保管される場所を保護するための、革新的な暗号化、クラス最高の暗号管理技術、強固な認証およびアイデンティティ管理ソリューションを活用することにより、主要な金融機関や政府機関を含む多くの業種でセキュリティに対してデータ中心のアプローチを取ることを可能にします。これらのソリューションを通して、ジェムアルトは、ますますデジタル化が進む世界において組織が顧客の信頼を守るために、厳しいデータプライバシーの規制などを遵守する手助けをし、企業の機密情報、顧客情報、電子取引を情報漏洩や改ざんから守ります。

技術仕様

オペレーティングシステム
- Windows, Linux, AIX, HP_UX, Solaris

暗号化API
- PKCS#11, CAPI/CNG, JCA/JCE, JCProv, OpenSSL

暗号処理

非対称アルゴリズム
- RSA（最大4096ビット）、DSA、ECDSA Diffie Hellman（DH）、ECC Brainpool曲線（名前指定およびユーザー定義）、その他

対称アルゴリズム
- AES、DES、3DES、CAST-128、RC2、RC4、SEED、ARIA、BIP32およびSECP256k1、Milenage、その他
- ECB、CBC、OFB64、CFB-8 (BCF)などのモードをサポート

ハッシュアルゴリズム
- MD5, SHA-1, SHA-256, SHA- 384, SHA- 512, MD2, RIPEMD128, RIPEMD160, DES MDC-2 PAD1

メッセージ認証コード
- SHA-1, SHA-256, SHA-384, SHA-512, MD2, RIPEMD128, RIPEMD160, DES MDC-2 PAD1, SSL3 MD5 MAC, AES MAC, CAST-128 MAC, DES MAC, DES3 MAC, DES3 Retail CFB MAC, DES30x9.19 MAC, IDEA MAC, RC-2 MAC, SEED MAC, ARIA MAC, VISA CVV

物理的特性

寸法
- 437 mm (W) x 270 mm (D) x 44 mm (H) (PSE2モデル)
- 482.6mm (W) x 533.4mm (D) x 43.815mm (H) (PSE2+モデル)

消費電力
- 220/110ボルト切り替え可能（PSE2モデル）
- 最大110W、通常43W（PSE2モデル）
- 220/110ボルト自動切り替え（PSE2+モデル）
- 最大180W、通常155W（PSE2+モデル）

温度
- 動作温度0°C～35°C

セキュリティ認定
- FIPS 140-2レベル3

安全および環境コンプライアンス
- UL, CSA, CE
- FCC, KC Mark, VCCI, CE
- RoHS, WEEE

お問い合わせ先：すべてのオフィスの所在地と連絡先情報につきましては、safenet.gemalto.jpをご覧ください。

フォローする：blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free