Entrust nShield HSMsがVerifoneのVeriShield Total Protectソリューションを保護

セキュアな電子POSソリューションのリーダーは、厳しい環境の中で、カード保有者のデータを処理拒絶からどのようにして守ることができたのでしょうか？

課題：パフォーマンスを低下させることなく、クレジットカードのトランザクションのセキュリティを最大化する

信頼されるセキュアな決済ソリューションのリーダーとして、Verifoneは、小売業者にはクレジットカードのトランザクションのセキュリティを確保し、顧客データの不正使用リスクを低下させる、より優れた方法が必要であると理解していました。大規模なデータ改ざんが次々と発生し、小売業者は毎年数百万ドルもの被害を被り、評判は傷つき、売上高は減少します。ただし、カード保有者のデータ保護を強化するどのソリューションを採用するにしても、その一方で処理業者や小売業者などのユーザーに対しては、1日に数百万件に上ることもあるトランザクションを処理する最高水準のパフォーマンスを維持する必要があります。

ソリューション: ENTRUST NSHIELD HSMsが提供するエンドツーエンドの暗号化

Verifoneは、VeriShield Total Protectソリューションの重要なコンポーネントとして高保証の暗号化と鍵管理機能を提供するEntrust nShield®ハードウェアセキュリティモジュール（HSMs）を検討しました。VeriShieldは、カードを受け付けたその瞬間から、処理時点、そしてトランザクションが復号化され、決済ネットワークに送信されるまで、カード保有者のデータを暗号化します。Entrust nShield HSMsを使用して、1件毎のトランザクションを保護するための安全な鍵交換と、特別な鍵を生成する安全な鍵導出を実行します。

VerifoneはEntrust nShield Security Worldアーキテクチャに固有の性能を活用して、冗長性を構築し、複数のデータセンターに実装された複数サーバと複数HSMsをシームレスに組み合わせ、ロードバランシングおよびフェールオーバーを自動化し、極めて高水準のトランザクション件数を処理することができます。さらに、Entrustを利用することで、Verifoneは顧客にオンサイト（通常）で、またはVerifoneがホストするマネージドサービスの一部として、HSMsをホストするオプションを提供できます。

詳細をチェック：ENTRUST.COM/ja/HSM

Verifone

このソリューションにより、Verifoneは、カード保有者のデータの悪意のある取得に対する強力なセキュリティとリスク低減という特異な組み合わせを実現する傍ら、パフォーマンスとトランザクションの可用性を確保するという、小売業者にとってウィン-ウィンの状況を生み出しています。さらに、エンドツーエンドの暗号化（ポイントツーポイント暗号化、P2PEとも言う）の実装によって、POS（受け入れ時点）と処理業者で復号化されるまでの間にある仲介システムについては、それを通過するデータは暗号化されているため、大半のPCI DSSコンプライアンス要件から除外されています。Verifoneのソリューションは、小売業者がPCI DSS要件を優に超えるセキュリティを提供できるようにすることを特に念頭に置いています。

ソリューションについて

Entrust nShield HSM

Entrust nShield HSMは、安全な暗号化処理、鍵の保護・管理を実行できるよう、強化された耐タンパ環境を提供します。このデバイスを使用することで、暗号化システムおよびプラクティスに対する注意義務の広く確立された基準と新しい基準を満たす、高保証のセキュリティソリューションを展開し、同時に高いレベルの運用効率を維持することができます。

Entrust nShield Connect HSMsは、組織の最も重要なアプリケーションの暗号化操作とそれに関連する鍵を分離し、保護します。Entrust nShield Connect HSMsは、公開鍵基盤（PKI）、ID管理システム、アプリケーションレベルの暗号化、トークン化、SSL/TLS、コード署名など、幅広い商用およびカスタムビルドのアプリケーションの暗号化、デジタル署名、鍵管理を実行します。ソフトウェアベースの暗号化ライブラリに代わる高保証のEntrust nShield Connect HSMsは、あらゆる主要アルゴリズムの証明された実装、世界最速のECCパフォーマンスなどを特長とします。

Entrust nShield HSMを使用することで、以下が可能になります。

- 耐タンパー性ハードウェア内で暗号鍵と操作に認定された保護を提供し、重要なアプリケーションのセキュリティを大幅に強化する。
- 従来のデータセンターおよびクラウド環境で、費用対効果の高い暗号高速化と他では見られない柔軟な運用を実現する。
- ソフトウェアのみを使用した暗号化のセキュリティ上の脆弱性とパフォーマンスの課題を克服する。
- コンプライアンス要件の遵守と、バックアップやリモート管理を含む日常の重要な管理タスクにかかるコストを削減する。Entrust nShield HSMを使用することで、必要な容量のみを購入し、要件の変化に応じてソリューションを簡単に拡張することができます。

Verifone

ENTRUSTを利用する理由は？

Verifoneは、3つの異なるベンダーが提供する6種類のHSMモデルを評価し、Entrust nShield Connect HSMsを選択しました。その選択には以下の理由がありました。

- **相互運用性および統合。**Entrustは複数のインターフェース（標準的なPKCS #11と低レベルのインターフェース）を提供したため、Verifoneのデベロッパーは、VeriShieldのアーキテクチャを最大限生かしてHSMを柔軟に統合できたこと。
- **使いやすさ。**Verifoneは、パフォーマンスを最大にし、鍵の持続性を最小化するシステムのアーキテクチャにおいて、Entrust nShield HSMsが使いやすく、他のHSMsよりもはるかに柔軟であることに気付いたこと。
- **性能：**Entrust nShield HSMsのスループットは、競合製品と比べてかなり多いため、Verifoneは小売業者にVeriShieldソリューションではパフォーマンスが劣化しないことを保証できたこと。
- **サポート**: Verifoneは、nShield HSMsのインストールにおけるEntrustチームとの緊密な協力体制や、Entrustのスペシャリストがデベロッパーに提供できる支援を評価したこと。
- **Entrust nShield Security World。**Entrust nShield Security Worldアーキテクチャにより、Verifoneチームは、適切なロードバランシング、高可用性、信頼性を提供するシステムを設定できたこと。それにより、VeriShieldが保護したトランザクションは、複数のサイトおよび複数のHSMsにわたって同時に処理できること。

詳細をチェック：ENTRUST.COM/ja/HSM

Verifone

主な利点

- 高保証の重要データの暗号化を実行し、パフォーマンスや可用性を犠牲にすることなく、ライフサイクル全体の鍵管理
- 自動化されたロードバランシングとフェースオーバーで高水準のトランザクション件数に対応
- PCI DSS要件を優に超えるセキュリティを提供
- 強力な鍵管理アーキテクチャにより、業務およびコンプライアンスレポート関連費用を削減
- 負担やリスクに晒されている管理タスクを自動化し、単一障害点や高価で手作業を必要とするバックアッププロセスを排除

ENTRUSTについて

Entrustは、信頼できるアイデンティティ、決済、データ保護を可能にすることにより、世界を安全に動かし続けます。今日、国境を越えた移動、買い物、電子政府サービスへのアクセス、企業ネットワークへのログインといったさまざまな場面で、シームレスで安全なユーザー体験がこれまで以上に求められています。Entrust はこうしたインタラクションの要となり、他にはない多様なデジタルセキュリティと認証発行ソリューションを提供しています。2,500人を超える従業員、グローバルパートナーのネットワーク、150か国以上に顧客を擁するEntrustは、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