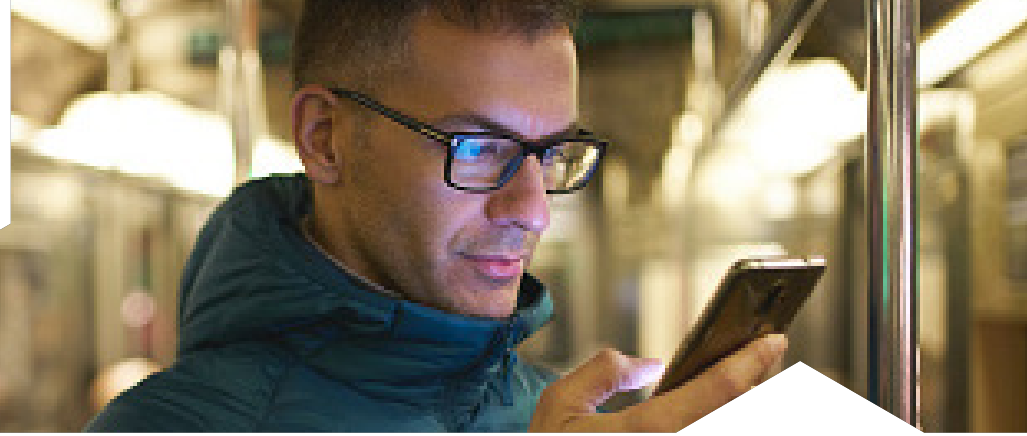




ENTRUST



Entrust nShield HSM は、Snapperのモバイルリロード トランジットソリューションの安 全性を確保します



革新的な企業が、鉄で覆われたセキュリティを提供しながら、通勤者に利便性をどのように追加したか。

課題：パフォーマンスを低下させることなく、モバイルトランジット購入のセキュリティを最大化する

ニュージーランドの進取的な企業であるSnapperは、アイルランドのダブリンで、乗客にとっての公共交通機関の改善に着手しました。アイルランド国立運輸局 (NTA) は、バスが視界に近づいているときにカードの読み込みができるようにすることで、乗客にとって交通費の支払いをはるかに便利にしたいと考えていました。Snapperは、NTAの顧客に対して、残高を確認し、スマートフォンを使用してLEAPTランジットカードを即座に再度読み込みする方法を提供する必要がありました。ソリューションは、最大500人の人々に同時にサービスを提供する必要があり、最大限のセキュリティを確保する必要がありました。

ソリューション：ENTRUST NSHIELD HSMによって保護されたスマートフォン決済

Snapperは、顧客がLEAPTランジットスマートカードをスマートフォンにタップし、Snapperのアプリ経由で支払いを行うことで、トランジットアカウントを読み込むことができるソリューションを設計しました。スマートフォンはカードに埋め込まれた非接触型チップを認識し、Snapperのアプリを開きます。アプリはカードを認証して読み取り、PCI準拠のクレジットカード取引を通して顧客をガイドします。その後、顧客はトランジットカードを使用して、ダブリンをバス、トラム、鉄道で移動します。

Snapperは、ソリューションのセキュリティを確保するために、Entrust nShield®ハードウェアセキュリティモジュール (HSM) を導入しました。Snapperのアプリは、顧客のトランザクションデータを暗号化し、Entrust nShield HSMを使用して、データの保護に不可欠な暗号化鍵を管理します。高いセキュリティを保証するために、暗号化されたすべてのデータはスマートカードの非接触型チップに保存されます。

CODESAFEはトランザクションの保護に役立ちます

Snapperのソリューションのセキュリティは、暗号化されたデータ、鍵の管理、および整合性を確保するためのスマートカードとHSM間の相互認証に依存しています。これらはすべてSnapperのカスタムルーチンによって駆動されます。この機密性の高いルーチンとそれが処理するデータは、クローズドシステムの外部に漏洩した場合、脅威に対して脆弱です。Entrust nShield CodeSafeは、Entrust nShield HSMの境界内で暗号コードを安全に保護することで、Snapperが必要とする保護を提供しました。

ENTRUST NSHIELD HSMは、顧客が鍵を制御できるようにします

NTAのマスターキーは最も価値のある秘密であり、NTAのITマネージャーは、それを保護するために非常に厳格なプロセスに従います。Entrust nShield HSMおよび関連するSecurity Worldアーキテクチャは、これらの鍵処理プロセスを完全にサポートし、NTAがSnapperの関与なしに、すべての本番鍵の関連機能を安全に管理することを容易にしました。

ENTRUSTのアーキテクチャは、厳格なポリシー遵守をサポートします

Entrust nShield Security Worldは、役割ベースの制御を実施することにより、権限のない担当者が暗号化鍵を制御するリスクを大幅に軽減するため、包括的なセキュリティの確保に役立ちます。

ソリューションについて

Entrust nShield HSM

Entrust nShield HSMは、安全な暗号化処理と鍵管理のために、耐タンパ環境を提供します。Entrust nShield HSMは認定されており、高い効率を維持しながら、暗号化システムの確立された新しいセキュリティ基準を満たしています。

Entrust nShield HSMは、組織の最も重要なアプリケーションの暗号化操作と鍵を分離して保護します。Entrust nShield HSMは、公開鍵基盤 (PKI)、SSL / TLS、コード署名など、幅広い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。Entrust nShield HSMは、ソフトウェアベースの暗号化に代わる高保証の代替手段であり、すべての主要なアルゴリズムをサポートし、世界クラスのECCパフォーマンスを備えています。

Entrust nShield HSMと独自のアーキテクチャを使用することで、必要な容量のみを購入し、ニーズ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。

Entrust nShield CodeSafe

Entrust nShield CodeSafeはnShield HSM内で機密性の高いカスタムアプリケーションをホストし、実行します。CodeSafeを使用することで、アプリケーションは安全な環境内でデータを復号化、処理、暗号化できます。その結果、スマートカードの認証に使用されるSnapperのコードなどのアプリケーションは、外部の脅威から十分に保護されます。

Entrust専門サービス

Entrust専門サービスセキュリティコンサルタントチームは、特定のビジネスニーズを満たすためにカスタマイズされたサービスを提供します。様々なアプリケーションの経験を持つ専門サービスチームは、組織が統合を計画し、リスクを軽減し、展開とフィールドテストを通じてプロジェクトを迅速かつ安全に実行するのを支援します。

ENTRUSTを利用する理由は？

Snapperは、6か月間に及ぶプロジェクトを開始しました。これは、別のセキュリティソリューションベンダーとの共同プロジェクトで、ニュージーランド国外への事業拡大において非常に重要であると考えていました。ベンダーはプロジェクト半ばで、暗号コードを保護したり、顧客であるアイルランド国家運輸局が要求するパフォーマンス仕様を実現するための要件を満たしていないことに気付きました。

あと3か月しかなく、SnapperはEntrustに介入するように依頼しました。Entrustのソリューションの選択が正しかった理由は？

- **実装しやすい** - Snapperは、設計とシームレスに統合できる簡単なソリューションを必要としていました。Entrustはこれを提供し、Snapperが固定予算内で、注目度の高い時間が限られたプロジェクトに成功するのを支援しました。
- **パフォーマンス** - Entrust nShield HSMは、プロジェクトが必要とする6倍の速度で、Snapperの元のセキュリティベンダーよりも大幅に速く、同時消費者トランザクションをサポートします。これにより、Snapperと国家運輸局は、消費者のニーズを満たすことに自信を持ち、成長の余地がありました。
- **エキスパートガイダンス** - Entrust専門サービスチームは、Snapperが「専門知識への摩擦のないアクセス」と呼ぶものを提供し、Snapperと効率的に連携して、プロジェクト要件に合わせてチームを調整し、Snapperがダブリンの運輸局にソリューションを迅速かつ自信を持って提供できるよう支援しました。

Entrustの主要なソリューションの利点

- 改ざん防止ハードウェア内で暗号化鍵および操作を保護し、ソフトウェアのみのソリューションよりもセキュリティを大幅に強化する。
- Entrust nShield CodeSafeを使用して、HSM境界内で機密性の高いカスタムアプリケーションを実行する。
- 独自のEntrust nShield Security World アーキテクチャを使用して、鍵管理を維持し、進化するニーズに応じて拡張可能なHSMセットを構築する。
- Entrust専門サービスチームのエキスパートガイダンスを受けて、効率的かつ自信を持ってソリューションを開発する。

ENTRUSTについて

Entrustは、信頼性の高い本人認証、決済、データ保護を可能にすることにより、世界の動きを安全に維持します。今日、人々はこれまで以上に、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を求めています。Entrustは、これらすべてのインタラクションに対応した、他では見られない広範なデジタルセキュリティおよび資格情報発行用ソリューションを提供しています。2,500名以上の従業員とグローバルパートナーのネットワークを備え、150か国以上における顧客から支持されているため、世界における多くの委託組織から信頼を得ていることは不思議ではありません。

詳細は下記URLをご覧ください。
entrust.com/ja/HSM

