Entrustは、Xumiのモバイル決済テクノロジー構築を支援

ビジネスにおけるチャレンジ

近距離無線通信（NFC）テクノロジーにより、近くに置かれた2台のデバイスは、データを交換することができます。近年、NFCテクノロジーにより、モバイルウォレットや非接触型カードを利用した非接触決済が可能になりました。

NFCを利用した決済は、消費者やマーチャントに新たな利便性をもたらす一方で、新しい不正手段にもなります。Xumiのプリンシパル、Juliana Cafik氏によると、モバイルウォレットやタッチ決済が主流になると、不正なNFC決済の比率が上昇します。不正な購入が起こる度に、商品が紛失し、マーチャントには高額のチャージバック手数料がかかります。

Xumiは不正な支払い取引が起こる前に止める、つまり、事実となった後で検知するのではなく、防止することを目標とする、セキュアな決済のプロバイダーです。同社のソリューションは、カード保有者とマーチャントの両方のセキュリティを強化するため、不正から保護する固有の複数レイヤーを採用しています。

> **当社の技術的な課題は、信頼できる実行環境（TEE）にアクセスしたり、新しいアルゴリズムや暗号理論を構築し、投資したりしなくても、クレジットカードを保存する安全な環境を消費者のスマートフォンに作ることでした。これがEntrust nShield HSMsが必要になる部分です。**
>
> – Xumiプリンシパル、Juliana Cafik氏

Xumi

Webベースの取引や実店舗での取引同様、モバイル決済では、消費者はクレジットカードを入れるウォレットが必要で、マーチャントは携帯端末のPOSが必要です。根底で使用されるテクノロジーは両方で一貫している必要があります。そして、どちらもセキュアである必要があります。

技術的な課題

Cafik氏は次のように語っています。「決済業界にはひびが入っています。カードまたは何らかのアカウントである消費者製品と、全く異なるテクノロジーで全く異なる当事者によってプロビジョニングされたトランザクションを受け取るマーチャントのアプリケーションの間には、システミックな分断があります。

この分断のため、消費者とマーチャントという2つの未知の当事者間の信頼を構築することが全くできません。そして、これこそが不正がこれほど多い原因なのです。これを修正する唯一の方法は、取引の両端を安全に処理する1つのテクノロジーを創造することです。

「当社の技術的な課題は、信頼できる実行環境（TEE）にアクセスしたり、新しいアルゴリズムや暗号理論を構築し、投資したりしなくても、消費者のスマートフォンでクレジットカードを保存する安全な環境を実現することでした。これが、Entrust nShield®ハードウェアセキュリティモジュール（HSMs）が必要になる部分です。」

ソリューション

nShield Connect HSMsは、強化された耐タンパ性ハードウェアデバイスであり、データの暗号化および復号や、デジタル署名とデジタル証明書の生成に使用される鍵を、生成、保護することにより、暗号化プロセスを強化します。Entrust nShield HSMsにより、企業は以下のことが可能になります。

- サイバーセキュリティに関する新しく設定された規制基準を満たし、それを上回る
- より高いデータの安全性と信頼性を実現する
- 高いサービスレベルとビジネスの機敏性を維持する

「当社には暗号化、認証、難読化コード、暗号理論、その他のテクノロジーなど、複数の保護措置があります」とCafik氏は言います。「ただし、Entrust nShield HSMsによって、当社はトランザクションの消費者とマーチャントの両側のためにアーキテクチャを形成することができます。それによって、携帯電話のTEEにアクセスすることなく、モバイルウォレットやモバイルの販売地点のセキュリティに新しい基準を作ります。」

「システムのセキュリティはモバイルアプリとサーバーの両サイドを対象とします。HSMは、私たちが両側の信頼を確認し、消費者の携帯端末から独立できるストラクチャを創造するのに役立っています。これは特にサーバ側に有益です。当社の主な目的は、不正な支払いから保護することで、サーバ側は保管された個人情報および決済情報の暗号化にPCIデータセキュリティスタンダード（PCI DSS）のセキュリティ要件を完全に満たし、高セキュリティ環境でオペレーションを設定する必要があります。これには、HSMsが不可欠です。当社はまた、サーバとクライアント間の通信をセキュアにし、設定情報のセキュリティを確保するためにもHSMsを使用しています。」

Xumi

> **Entrustの営業チームはこのプロジェクトに大きく貢献しました。このチームは知識が豊富で、丁寧に順を追って当社を成功に導きました。**
>
> – Xumiプリンシパル、Juliana Cafik氏

Cafik氏によれば、信頼の基点を提供するEntrust nShield Connect HSMは、初期の段階から設計の一部を担い、全体的な運用環境のセキュリティの要となっています。

結果

Xumiは、パートナー企業であるCyberSourceとGlobal Paymentsとともに、モバイル決済アプリケーションの商業的な概念検証を進めています。Xumiのアプリケーションは既にOpen Web Application Security Project（OWASP）のレベル2の認証を受けています。OWASPのアプリケーションセキュリティ検定基準（ASVS）プロジェクトは、webアプリケーションの技術的なセキュリティ制御のテスト基準を提供し、デベロッパーにセキュアな開発要件のリストを提供するものです。[1]

Xumiは概念検証を完了した後、バックアップサイトにさらにEntrust nShield HSMsを実装し、完全なディザスタリカバリ、ホットフェイルオーバー、ロードバランシングを実現します。同社は今後もEntrustの専門家と協力し、迅速な取引に最大限の対応力を確保します。

Cafik氏は述べています。「Entrustの営業チームはこのプロジェクトに大きく貢献しました。このチームは知識が豊富で、丁寧に順を追って当社を成功に導きました。振り返ってみると、チームが当社に楕円曲線暗号の使用を推奨したことに感謝しています。その推奨の成果を今、目の当たりにしています。」

「Entrustチームは、当社がまさに必要としていたものを最初から提供しました。それは当社のような企業にとって、極めて大きな利点です。当社は小規模です。当社の極めて優秀なデベロッパーは数人体制です。そのHSMが様々なコンフィグレーションを行ったり来たりしていたら、当社には非常に困難だったことでしょう。

チームは非常に思慮深く、当社がHSMをどのように活用しようとしているかを理解しようと努め、当社が直面するかもしれない問題を事前に予想しました。チームは当社の時間を無駄にしませんでした。私はそのことにとても感謝しています。」

Xumi

ビジネスニーズ

- 消費者とマーチャントの両方のセキュリティ要件を取り入れたモバイル決済テクノロジー

技術的ニーズ

- 消費者のモバイルデバイスとマーチャントの決済アプリケーションの間に直接信頼を可能にするセキュアなテクノロジーを創造する

ソリューション

- nShield Connect XC HSMs
- Entrustの専門家のサポート

技術的ニーズ

- 携帯デバイスのTEEにアクセスすることなく、トランザクションの消費者とマーチャントの両方にアーキテクチャを創造する
- セキュアなクライアントサーバ通信およびコンフィグレーション情報
- トランザクションのマーチャントサーバ側のPCI DSS要件遵守
- 商業的な概念検証の時間短縮

ENTRUSTについて

Entrust は信頼される認証、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、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。

[1]https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

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

Entrustは、米国およびその他の国におけるEntrust Corporationの商標、登録商標、またはサービスマークです。
©2020 Entrust Corporation.