Fastcomが高レベルのセキュリティを維持しながらコード署名の効率を向上

www.fastcom-technology.com

課題：FOXTELが競争力を維持できるようサポートする、より優れたセットトップボックス

有料テレビ市場は非常に競争が激しく、消費者は常に新たなコンテンツへのアクセスを求めています。Foxtelが有料テレビ市場をリードしているオーストラリアでさえも、Foxtelは、新規参入するオペレーターに対抗するために、新たなイノベーションの創造にさらに集中的に取り組み、優れた加入者体験を提供し続ける必要があります。

Foxtelは、強化されたコンテンツストリーム、より多くの録画スペース、加入者の満足度高向上を目的としたその他の新機能を提供する、iQ3セットトップボックス（STB）を発表しました。

iQ3を設計するにあたり、FoxtelはFastcomと提携し、中核的な要件を3つ特定しました。具体的には、STBに次の機能を搭載する必要がありました。

- マルチベンダー型のセキュリティ戦略をサポートして、Foxtelが複数のコンテンツプロバイダーによるストリーミング配信を提供し、必要に応じてプロバイダーを変更できるようにする
- サブスクリプション限定コンテンツへの不正アクセスを防止する
- Foxtelが展開されたデバイスを直接制御できるようにし、顧客のニーズに対応する効率的な更新を可能にする

ソリューション：ENTRUSTにより使用可能になったFASTCOM MCAS

Fastcomは、Foxtelのニーズに基づいて、複合型限定受信システム（MCAS）ソリューションの初期仕様を開発する中で、システムには、STBの製造から始めて、安全性の高い暗号化機能を搭載する必要であるとすぐに認識しました。実際に、デバイス上で行われるすべての暗号化処理と復号処理に信頼の基点を提供するルート鍵を、iQ3の中核となるプロセッサに焼き付けることで、各デバイスのIDを確立し、限定受信システム（CAS）やデジタル著作権管理（DRM）ソリューションのコンテンツを暗号化するための鍵の作成を可能にする必要がありました。

Fastcom

Fastcomは、アプリケーションが要求するレベルのセキュリティを実現するために、FIPS認定の環境内で鍵導出アルゴリズムを実行する必要があると判断しました。Fastcomは、ハードウェア・セキュリティ・モジュール（HSM）に精通しており、必要なセキュリティとモジュール性の提供において実績がありました。

Fastcomは、さまざまなベンダーの製品について検討した結果、プロジェクトのセキュリティ要件をすべて満たす比類のない性能を備えていることから、Entrust nShield® HSMを選択しました。具体的には、nShield CodeSafeは、Fastcomが独自の派生アルゴリズムを実行し、FIPS140-2レベル3認定の境界内で鍵を保護できるようにする、比類のない機能を備えています。

実装段階において、EntrustチームはCodeSafe環境内で暗号化アプリケーションコードの一部を開発し、その後、Fastcomがそれをさらなる改良を加えました。これにより、Fastcomは、中核コードの所有権を簡単に引き継ぐと同時に、ソリューション構築の最初の一歩を踏み出すことができました。

nShield HSMを使用するFastcomが、単一のルート鍵から複数の従属鍵を取得し、FoxtelがそれをiQ3STBに組み込みます。これらの鍵は、CASベンダーがCASまたはDRMソリューションを通じて提供されるコンテンツを暗号化するために使用され、特定のSTBでのみコンテンツをレンダリングできるようにします。

Entrust nShield HSMがMCASソリューションの土台となることで、FoxtelはiQ3 STBのアプリケーション、ミドルウェア、CASまたはDRMソリューションを自由に選択することができます。これにより、マルチベンダー型アプローチ、必要に応じたSTBの効率的かつ低コストでの更新、有料テレビ加入者へのプレミアムコンテンツの配信が可能になります。Fastcomは将来的に、MCASモデルを使用して、マルチベンダー型セキュリティアプローチを活用する、その他の顧客宅内通信機器ソリューションを開発したいと考えています。

主なメリット

- コストのかかるSTBの更新を行う必要がなく、CASベンダーやミドルウェアを簡単に変更可能
- リモートで展開されたデバイスを直接制御して、加入者体験を向上
- プレミアムコンテンツを保護することで収益源を維持

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 HSMは、独立した認証機関によって認定されており、ユーザが自信を持ってコンプライアンスの義務と社内ポリシーに対応できるようにする、定量化可能なセキュリティベンチマークを確立します。Entrust nShield HSMは、さまざまなフォームファクタで利用でき、ポータブルデバイスから高性能データセンターアプライアンスに至るまで、あらゆる一般的な展開シナリオをサポートします。

Fastcom

ENTRUST CODESAFE

Entrust CodeSafeデベロッパーツールキットは、FIPS140-2レベル3認定を受けたnShield HSMの保護された境界内で、機密性の高いアプリケーションを移動する独自の機能を提供します。このアプローチを使用すると、アプリケーションの改ざんを防止し、安全な環境内でデータを復号、処理、暗号化することができます。

CODESAFEにより、企業は以下が可能になります。

- 環境を問わず機密性の高いアプリケーションのリモート管理を提供し、またサーバでもメインフレームでも、顧客が使用するOSや構成に関係なく暗号化サービスを提供することにより、**知的財産の盗難を防ぐ**。CodeSafeを使用することで、アプリケーションまたはハンドヘルドデバイスの所有者は、物理的なプレゼンスなく、最新のアプリケーションの実行環境を維持できます。
- 信頼できるアプリケーションにデジタル署名する機能を提供することにより、ハッカーや不正な管理者による**攻撃からアプリケーションを保護**し、起動前にアプリケーションの整合性を検証する。CodeSafeはまた、アウトソーシングと契約を利用する制御されていない環境でも、アプリケーションを盗難から保護します。
- 真のエンドツーエンドSSL暗号化を提供し、SSLを終了し、HSM内で機密データを処理して攻撃から保護することにより、**機密SSLデータを保護する**。

FASTCOMについて

スイスの独立企業であるFastcomは、有料テレビ市場においてセキュリティソリューションと技術コンサルティングを提供しています。

FastcomのMCASソリューションには、有料テレビのセットトップボックス（STB）といった顧客宅内通信機器向けの、さまざまなライセンシング機関サービスが統合されています。MCASは、スケーラブルなモジュラー型インフラストラクチャを活用して、複数の限定受信システム（CAS）ソリューションやデジタル著作権管理（DRM）ソリューションを同時にサポートすると同時に、有料テレビ事業者による現場でのSTBの直接制御を可能にします。

FOXTELについて

Foxtelはオーストラリアの主要メディア企業であり、オーストラリア国内の280万以上の家庭に、有料テレビおよびインターネットサービスを提供しています。

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、支払いや国際取引、電子政府サービスへのアクセス、そして企業ネットワークへの認証において世界中でより安全で円滑なユーザ体験が求められています。Entrust はこれらの要となる部分において、他に類を見ない幅広いデジタルセキュリティとID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ネットワーク、そして150カ国以上におよぶ顧客に支えられ、世界で最も信頼されている組織から信頼されています。

Fastcom

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
- 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
- ソフトウェアのみを使用した暗号化に見られる、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
- 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。Entrust nShield HSMs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

ENTRUSTが選ばれた理由とは？

- Entrustは、豊富な専門知識に裏打ちされた実装実績と、nShield HSMが提供するセキュリティおよび独自の機能により、このビジネスチャンスを勝ち取りました。

EntrustがFastcomにもたらしたメリット

- 業界をリードするセキュリティ。Fastcomは、iQ3 STBの現場への導入後、プレミアムコンテンツを不正アクセスから保護するにあたり、Foxtelが信頼することができるソリューションを提供する必要があることを認識していました。MCASソリューションは、Entrust nShield HSMを中核として、最高レベルのセキュリティと機能を提供します。
- 暗号化アルゴリズムを実行するための保護された環境。Fastcomは、業界最高レベルの保護が必要とする、独自の鍵導出アルゴリズムを開発しました。Entrust CodeSafeは、アプリケーションをHSMのFIPS認定境界内で実行できるようにする唯一のソリューションであり、標準のサーバーベースのプラットフォームで蔓延する攻撃からアプリケーションを保護します。
- 高度なセキュリティに関する専門知識。Entrustのプロフェッショナルサービスチームの専門家がFastcomと提携し、iQ3 STBを保護する信頼の基点となる鍵を導出するアプリケーションの構築を開始しました。Fastcomはこれを足がかりとして、MCASソリューションの開発を促進しました。

mcas

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