



ENTRUST



# PRIMA Cinemaは EntrustnShield HSMを使用して、 初上映映画の新しい市場を開拓します

PRIMA<sup>TM</sup>  
CINEMA

メディア会社がスタジオのセキュリティ上の懸念をいかに乗り越えて、新しくリリースされた映画をホームシネマに直接配信するか。

**課題：リリースされたばかりの映画を家庭の視聴者に直接配信するための安全な方法を開発する**

PRIMA Cinemaの創設者は、新しい市場機会を利用して、リリースされたばかりの映画をホームシネマシステムを使用する顧客に提供すると同時に、映画が映画館で上映されることを望んでいました。映画館ではなく、自宅での映画鑑賞に関心を持つ人々の数が着実に増加しているため、毎年建設される高級ホームシアターの数は急速に増加しています。PRIMA Cinemaチームは、最大のハードルであるセキュリティの問題を解決できれば、映画館のような品質の映画をホームシネマに配信することで競争優位性を得ることができると感じました。

映画の著作権侵害は、映画やテレビの所有物が違法にコピーされて配信されると、毎年数十億ドルを失うと言われるスタジオや配給業者にとっては、大きな懸念事項です。映画が映画館で上映される場合、映画館の管理者は「カミング」(ビデオカメラを使用して映画館で映画を録画する)を防ぐために観客を監視できますが、ホームシアターの場合は別のタイプのセキュリティが必要になります。PRIMAチームは、スタジオやその他のコンテンツ所有者からビジネスモデルの賛同を得るためには、視聴者体験を低下させることなく、映画を配給・上映するための安全性の高い方法を考案する必要があることを知っていました。

## ソリューション: ENTRUST NSHIELD HSMを使用した複数の暗号化レイヤー

スタジオや配給業者の懸念に対処するために、PRIMA Cinemaは、Entrust nShield®ハードウェアセキュリティモジュール (HSM) を使用して、プライベート暗号化およびデジタル署名鍵を生成して保護することで、複数レイヤーの暗号化とサーバーとホーム再生デバイス間の強力な認証を含む、映画をエンコードしてホームシアターに配信するシステムを開発しました。

PRIMA Cinemaは配信前に、HSMによって生成された256ビットのAES鍵を使用して映画を暗号化します。ホームシネマにインストールされている再生デバイスには、復号化とデバイス認証に関連する秘密鍵と証明書が保護・管理されるトラステッド・プラットフォーム・モジュール (TPM) が含まれています。

鍵が生成中にHSMや使用デバイスの外部に漏洩することはありません。すべての暗号化処理と鍵処理を制御するアプリケーションは、独自のnShield CodeSafe機能を使用してHSMのセキュリティ境界内で実行されます。すべてのnShield HSMに共通のnShield Security Worldの役割ベースのアクセス機能により、システムへのインサイダー攻撃の可能性を防ぐために、適切な複数人による管理制御が実施されます。映画はブロードバンド経由で再生デバイスに転送され、双方向の証明書ベースの認証で保護されます。さらに、再生デバイスに組み込まれた生体認証指紋リーダーにより、登録された真の所有者のみが実際にスクリーニングを開始できます。最後に、再生時に、セッション固有の透かしがHSMによって生成され、映画が録画されないよう、動画に目に見えないマークを付けるために使用されます。

PRIMA Cinemaのセキュリティへのアプローチは、独立したレビューを受け、コンテンツプロバイダーの非常に厳しい要件を満たしていることがわかりました。これにより、同社は、劇場公開された映画の使用許可とこれを個人のホームシアターに配信する権利を付与された映画館史上初の企業として市場に参入することができました。

## ソリューションについて

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、ユーザーにコンプライアンスの義務と社内ポリシーに対応できる自信を与える、定量化可能なセキュリティベンチマークを確立しています。Entrust nShield HSMは、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のすべての一般的な展開シナリオをサポートするために、複数のフォームファクタで利用できます。

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

- 改ざん防止ハードウェア内で暗号化鍵および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
- 費用対効果の高い暗号化アクセラレーションとクラウド環境を実現する
- 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

- 規制遵守と、バックアップやリモート管理を含む日常の主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

## NSHIELD CODESAFE

nShield CodeSafe デベロッパーツールキットは、FIPS140-2レベル3認定の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化、処理、暗号化することができます。

**nShield CodeSafeにより、組織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。 nShield 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の所有者は、物理的に存在することなく、最新のアプリケーション実行環境を維持することができます。
- 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。 nShield 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においても、アプリケーションを盗難から保護する。

- 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。

## ENTRUSTを利用する理由は？

Entrustは、以下を提供するnShield HSMのセキュリティと機能に基づいてビジネスを勝ち取りました。

- **優れたセキュリティ。** PRIMA Cinemaチームは当初から、スタジオから承認を得るには、本質的にリスクの高い標準アプリケーションプラットフォームを使用するのではなく、FIPS認定の強化されたアプライアンスアプローチの高保証セキュリティが必要であることを知っていました。 PRIMA Cinemaはまた、システムをレビューする人が誰でもその信頼性とセキュリティの実績にすぐに満足できるように、セキュリティ認証を備えた実証済みのソリューションを必要としていました。また、業界標準のアルゴリズムと、利用可能な最強の保護に適した鍵の長さを使用した、セキュリティへのマルチレイヤーアプローチを望んでいました。 Entrust nShield HSM確実に任務を果たしました
- **nShield CodeSafe。** Entrust nShield HSMは他のソリューションにはないセキュリティ機能を提供します。 CodeSafeを使用すると、アプリケーションをHSM内の安全な環境で実行できるため、標準のサーバ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できます。 PRIMA CinemaはCodeSafeを使用して、すべての鍵処理と暗号化・復号化操作を実行し、可能な限り最高レベルのセキュリティを提供しました。

## 主な利点

- 信頼できる環境内でセキュリティ機能を実行する代わりに、標準のアプリケーションプラットフォームでセキュリティ機能を実行する際の脆弱性を克服する
- 重要なアプリケーションや暗号化鍵および署名鍵を改ざん、マルウェア、トロイの木馬から保護する
- HSM暗号化サービスが様々な接続デバイスをサポートできるようにする
- FIPS140-2レベル3承認済みの改ざん防止ハードウェアで認定された保護を提供する
- 鍵管理タスクのコストを削減する

- **nShield Security Worldアーキテクチャ。**  
nShield Security Worldアーキテクチャは、鍵管理を合理化し、PRIMAがすべての厳格なセキュリティを容易に定義し、必要なプロジェクトを制御できるようにすることで、システム全体を構築かつ管理できるようにしました。Security Worldアーキテクチャは、統一された管理者/ユーザー体験を提供し、展開するデバイスが1台でも100台でも、その数を問わず、相互運用性を保証します。
- **優れたユーザー体験。** Entrust nShield HSMは、ユーザー体験の質を妨害したり損なったりすることなく、スタジオに必要な強力なセキュリティを透過的に提供することができました。これは、PRIMA Cinemaの価値提案において絶対に必要なことでした。

## 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](https://entrust.com/ja/HSM)

