Qube Cinemaは、Entrust nShield HSMを利用して、デジタルシネマ配信に革命をもたらします

デジタルシネマテクノロジーのメーカーが、最高レベルの信頼できるコンテンツ保護を提供することにより、デジタルシネマ配信のオンライン鍵管理でいかに市場を独占したか。

Qube Cinemaは、デジタルシネマ用のサーバ、プロジェクタ、マスタリング、配信テクノロジーのメーカーとして、映画業界が物理的配信からデジタル配信への10年にわたる移行を完了しつつあるときに、大きな混乱を起こさせるようなテクノロジーを市場に投入するというユニークな機会を得ました。デジタルには多大なメリットがありました。ハードドライブの製造と配送は、フィルムプリントの複数のリールよりもはるかに安価でした。デジタル映画はかなり速く配信できるため、配給業者は需要を満たしやすくなります。デジタル映画は時間の経過とともに劣化することはなく、また熟練度の低いスタッフが映すことも可能です。

最大のハードル、および映画産業がアナログからデジタルへの移行において他の産業に遅れをとった理由は、セキュリティの問題でした。映画制作会社であるコンテンツ所有者は、著作権侵害について非常に懸念しており、非常に高いレベルのセキュリティ対策を求めていました。一方、映画館所有者と配給業者は、収益性を損ない、運営上の負担をもたらすような複雑で費用のかかるセキュリティ対策を取らなければならないことを望みませんでした。Qubeチームは、最高レベルのセキュリティを備え、かつ操作が非常に簡単なデジタル映画の鍵をオンラインで管理するための効率的な方法を見つけることができれば、映画業界に革命を起こすことができることを知っていました。

Qube Cinema

ソリューション：KEYSMITH：ENTRUST NSHIELDを使用したオンライン鍵管理システム

Qube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、業界で利用可能な最高レベルのセキュリティを備え、かつ使いやすい配信システムを開発しました。デジタルシネマでは、映画はデジタルシネマパッケージ（DCP）にエンコードおよび暗号化され、ハードドライブまたは衛星フィードを介して配信されます。その後、特定の映画館、時間枠、上映回数に応じて、映画のロックを解除する一意の鍵配信メッセージ（KDM）に含まれる情報を使用して、映画館で復号化できます。

KeySmithは、コンテンツの所有者と配信者の両方の要件を満たしています。コンテンツ所有者は、配信者が通常使用するソフトウェアベースの社内暗号化対策や、暗号化鍵を紛失して自分のコンテンツからロックアウトされるという最悪のシナリオについて心配する必要がなくなりました。Entrust nShield HSMは、業界で最高レベルのコンテンツ暗号化鍵の保護を提供すると同時に、鍵の紛失を防ぎます。配給業者と映画館所有者に対して、Qubeシステムは、高度なセキュリティを実装する際の障壁や、利便性のためにセキュリティを犠牲にしたいという誘惑を取り除くレベルの操作の容易さも提供します。

システムの仕組みは次のとおりです。スタジオまたは独立した映画制作会社が映画配給に向けて提出してします。これは、映画を構成するメディアファイルとメタデータの業界標準形式であるDCP（デジタルシネマパッケージ）に変換されます。DCP内で、一連のAES鍵が個々のファイルを暗号化するために使用されます。これらの鍵を安全に伝送する配信KDM（DKDM）は、配信者のKeySmithアカウントで利用できるようになります。このDKDMにより、KeySmithは個々の映画館のKDMを生成できます。Entrust nShield HSMは、KeySmith内で各企業に固有のRSA公開／秘密鍵ペアと関連するデジタル証明書を作成します。このHSMは、HSMの認定されたセキュリティ境界内で実行されるアプリケーションを使用して、受領者の映画館の公開鍵でAES鍵を暗号化します。本来の受領者のみが、生成時に一意で安全にインストールされた関連する秘密鍵を使用して、パッケージを復号化できます。KeySmithは、KDMを映画館に直接配信することもできます。これは通常、映画館がハードドライブまたは衛星ダウンロードを介して映画を受領した後に行われます。これは非常に効率的なシステムであり、配給業者に使いやすさを提供すると同時に、映画コンテンツの高保証の保護を確実にします。これは、Qubeのビジネス価値提案の2つの重要な要素です。

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。

Qube Cinema

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。
- 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。
- 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。

ENTRUST NSHIELD CODESAFE

CodeSafeデベロッパーツールキットは、認定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。FIPS 140-2レベル3 HSMで安全に読み込まれ、実行されるアプリケーションは、改ざんから保護され、安全な環境内でデータを復号化、処理、および暗号化できます。

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。CodeSafeを使用することで、アプリケーションの所有者は、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**。

ENTRUSTを利用する理由は？

Entrustを使用するというQubeの決定は、次のいくつかの主要な要因の影響を受けました。

- **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。Qube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。
- **信頼性と評判**。Qubeは、スタジオや映画業界から信頼を獲得するには、最高レベルの精査に耐られる最も信頼性および信憑性が高いセキュリティソリューションを選択する必要があることを知っていました。Entrust nShield HSMは実証されたパフォーマンス、改ざん防止ハードウェア、暗号化鍵のFIPS 140-2レベル3認定保護を備え、法案に完全に適合します。

Qube Cinema

主な利点

- 信頼できる環境内で実行することにより、ホスト側アプリケーションのセキュリティの脆弱性を克服する
- 重要なアプリケーションを改ざん、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

- **強靭性と可用性**。Entrust nShield HSMはQubeが配給業者への鍵の可用性を確保できるようにします。これは、このサービス業界で信頼を構築するための重要な側面です。Entrust nShield HSMを地理的に複数の場所で実行して強靭性を確保することで、Qubeは鍵を容易にバックアップし、複数のHSMの同期を維持して、グローバルユーザーに鍵を提供することができます。

- **拡張性**。Entrust nShield HSMにより、Qubeは無制限の数の鍵を発行し、管理することができます。これは、Qubeがデジタルシネマプロバイダーに提供するオンラインサービスの潜在的な成長にとって重要です。

- **反応性**。Qubeは、Entrustから受けたプレセールおよびアフターセールのサービスとサポートのレベルに感銘を受けました。

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

ENTRUST

お問い合わせ：
HSMinfo@entrust.com