Qube Cinema revolutioniert mithilfe von Entrust nShield-Hardware-Sicherheitsmodulen (HSMs) den digitalen Kinovertrieb

Ein Höchstmaß an Sicherheit sorgte dafür, dass ein Hersteller von Digitalkinotechnologie zum Marktführer für die Online-Schlüsselverwaltung beim Vertrieb digitaler Kinofilme wurde.

Als Hersteller von Servern, Projektoren sowie Mastering- und Distributionstechnologie für digitales Kino sah Qube Cinema eine einzigartige Gelegenheit, eine disruptive Technologie auf den Markt zu bringen – zu einem Zeitpunkt, als die Filmindustrie dabei war, den jahrzehntelangen Übergang vom physischen zum digitalen Vertrieb zu vollziehen. Die digitale Distribution bietet enorme Vorteile, da es viel kostengünstiger ist, Festplatten herzustellen und zu versenden als Rollen um Rollen von Film. Zudem sind digitale Filme viel schneller an Ort und Stelle, sodass Verleiher die Nachfrage besser befriedigen können. Digitale Filme verlieren im Laufe der Zeit auch nicht an Qualität, und sie können von weniger qualifizierten Arbeitskräften projiziert werden.

Die größte Hürde und der Grund dafür, dass die Filmindustrie bei der Umstellung von analog auf digital hinter anderen Branchen hinterherhinkte, war die Sicherheit. Filmproduktionsfirmen als Eigentümer der Inhalte hatten extreme Sicherheitsbedenken angesichts Piraterie und verlangten sehr hohe Sicherheitsmaßnahmen. Kinobesitzer und Verleiher hingegen wollten sich nicht mit komplizierten oder kostspieligen Sicherheitsmaßnahmen auseinandersetzen müssen, die der Rentabilität schaden und operative Belastungen mit sich bringen würden. Das Qube-Team wusste, dass es die Branche revolutionieren könnte, wenn es einen effizienten Weg finden würde, mit dem digitale Kinoschlüssel mit dem höchsten Sicherheitsgrad in einer Onlineumgebung verwaltet werden können, solange dabei eine einfach Handhabung garantiert bleibt.

Qube Cinema

DIE LÖSUNG: KEYSMITH: EIN ONLINE SCHLÜSSELVERWALTUNGSSYSTEM AUF BASIS VON ENTRUST NSHIELD HARDWARE-SICHERHEITSMODULEN(HSMs)

Um dem Bedarf an effizienter Sicherheit bei der Distribution digitaler Kinoinhalte gerecht zu werden, nutzte Qube Entrust nShield® Hardware-Sicherheitsmodule (HSMs), um ein einfach zu bedienendes Distributionssystem mit dem höchsten in der Branche verfügbaren Sicherheitsniveau zu entwickeln. Digitales Kino bedeutet, dass Filme in einem Digital Cinema Package (DCP) kodiert und verschlüsselt und über eine Festplatte oder eine Satellitenverbindung distribuiert werden. Anschließend werden sie im Kino mithilfe von Informationen entschlüsselt, die in einer einzigartigen Key Delivery Message (KDM) enthalten sind. Damit wird der Film für ein bestimmtes Kino, einen bestimmten Zeitraum und eine bestimmte Anzahl von Vorstellungen freigeschaltet.

KeySmith erfüllt die Anforderungen von Inhaltseigentümern und Distributoren gleichermaßen. Inhaltseigentümer müssen sich keine Sorgen mehr über die softwarebasierten, hausinternen Verschlüsselungsmaßnahmen machen, die typischerweise von Distributoren verwendet werden, oder über das schlimmste Szenario – den Verlust der Verschlüsselungsschlüssel und aus den eigenen Inhalten ausgesperrt zu sein. Die Entrust nShield HSMs bieten den branchenweit höchsten Grad an Schutz für Schlüssel zur Inhaltsverschlüsselung und stellen gleichzeitig sicher, dass Schlüssel niemals verloren gehen. Für Verleiher und Kinobesitzer bietet das Qube-System auch ein Maß an Bedienungskomfort, das alle Hindernisse bei der Implementierung hoher Sicherheit beseitigt und damit auch jegliche Versuchungen, die Sicherheit der Bequemlichkeit zuliebe zu opfern.

So funktioniert das System: Ein Studio oder ein unabhängiger Filmemacher reicht einen Film zum Verleih ein. Dieser wird in ein DCP (Digital Cinema Package) konvertiert – das Industriestandardformat für die Mediendateien und Metadaten, aus denen ein Film besteht. Innerhalb des DCP wird ein Satz von AES-Schlüsseln verwendet, um einzelne Dateien zu verschlüsseln. Eine DKDM (Distribution Key Delivery Message), die diese Schlüssel sicher trägt, wird dann dem KeySmith-Konto des Distributors zur Verfügung gestellt. Diese DKDM ermöglicht es KeySmith, KDMs für einzelne Kinos zu generieren. Entrust nShield HSMs erstellen innerhalb von KeySmith für jedes Unternehmen ein eindeutiges RSA-Schlüsselpaar aus einem öffentlichem und privatem Schlüssel mit einem dazugehörigen digitalen Zertifikat. Diese HSMs verschlüsseln die AES-Schlüssel mit dem öffentlichen Schlüssel des Empfängerkinos unter Nutzung einer Anwendung, die innerhalb der zertifizierten Sicherheitsgrenze des HSM läuft. Nur der vorgesehene Empfänger kann das Paket mit dem zugehörigen privaten Schlüssel entschlüsseln, der bei der Herstellung einmalig und sicher installiert wird. KeySmith kann die KDMs auch direkt an die Kinos liefern. Dies geschieht in der Regel, nachdem die Kinos den Film per Festplatten- oder Satelliten-Download empfangen haben. Das Ganze ist ein hocheffizientes System, das den Verleihern eine einfache Handhabung bietet und gleichzeitig einen hochsicheren Schutz der Filminhalte gewährleistet, was zwei entscheidende Elemente des Kundenangebots von Qube sind.

ÜBER DIE LÖSUNG

Entrust nShield HSMs bieten eine gefestigte, manipulationssichere Umgebung für sichere kryptographische Verarbeitung, Schlüsselschutz und Schlüsselverwaltung. Mit diesen Geräten können hochsichere Lösungen eingesetzt werden, die etablierte sowie neue Sorgfaltsstandards für kryptographische Systeme und und Praktiken erfüllen, während gleichzeitig ein hohes Maß an betrieblicher Effizienz beibehalten wird.

Entrust nShield HSMs sind von unabhängigen Behörden zertifiziert und legen quantifizierbare Sicherheits-Benchmarks fest, sodass Kunden sich darauf verlassen können, dass Compliance-Vorgaben und interne Richtlinien eingehalten werden. Entrust nShield HSMs sind in verschiedenen Formfaktoren erhältlich, um alle gängigen Einsatzszenarien von tragbaren Geräten bis hin zu Hochleistungs-Rechenzentrumsgeräten zu unterstützen.

Qube Cinema

Mit Entrust nShield HSMs können Sie

- zertifizierten Schutz für kryptographische Schlüssel und Abläufe innerhalb manipulationssicherer Hardware bereitstellen, der die Sicherheit kritischer Anwendungen deutlich erhöht,
- in herkömmlichen Rechenzentren und Cloud-Umgebungen kryptographische Abläufe kostengünstig beschleunigen und beispiellose operative Flexibilität erreichen,
- die Sicherheitslücken und das mangelnde Leistungsvermögen einer Kryptographielösung, die rein softwarebasiert ist, hinter sich lassen, und
- die Kosten für die Einhaltung gesetzlicher Vorschriften und die täglichen wichtigen Verwaltungsaufgaben einschließlich Back-up und Fernverwaltung senken. Sie kaufen nur die Entrust nShield HSMs, die Sie aktuell benötigen. Sollten Ihre Anforderungen zunehmen, können Sie die Kapazität Ihrer Lösung jederzeit anpassen.

ENTRUST NSHIELD CODESAFE

Das CodeSafe Entwickler-Toolkit bietet die einzigartige Möglichkeit, sensible Anwendungen innerhalb des geschützten Umkreises eines zertifizierten nShield HSM zu verschieben. Anwendungen, die sicher auf HSMs nach FIPS 140-2 Level 3 geladen und ausgeführt werden, sind vor Manipulationen geschützt und können Daten innerhalb dieser sicheren Umgebung entschlüsseln, verarbeiten und verschlüsseln.

Vorteile von CodeSafe für Unternehmen:

- **Der Diebstahl geistigen Eigentums wird verhindert**, indem die Fernsteuerung sensibler Anwendungen unabhängig von der Umgebung ermöglicht und kryptographische Dienste unabhängig vom Betriebssystem oder der Konfiguration des Kunden, ob Server oder Mainframe, angeboten werden können. CodeSafe ermöglicht es Anwendungseigentümern außerdem, die Anwendungsausführungsumgebung ohne physische Anwesenheit auf dem neuesten Stand zu halten.
- **Anwendungen werden vor Angriffen durch Hacker oder betrügerische Administratoren geschützt,** da vertrauenswürdige Anwendungen digital signiert werden können, sodass ihre Integrität vor dem Start überprüft wird. CodeSafe schützt Anwendungen auch vor Diebstahl, selbst in nicht kontrollierten Umgebungen, wo mit Outsourcing und Auftragsvergabe gearbeitet wird.
- **Schutz sensibler SSL-Daten vor Angriffen** durch eine echte End-to-End-SSL-Verschlüsselung, die Beendigung von SSL und die Verarbeitung sensibler Daten innerhalb des HSM.

WARUM ENTRUST?

Die Entscheidung von Qube für Entrust wurde von mehreren wichtigen Faktoren beeinflusst:

- **CodeSafe**. Entrust nShield HSMs bieten eine Sicherheitsfunktion, die keine andere Lösung bietet: Mit CodeSafe können Anwendungen in einer sicheren Umgebung - innerhalb des HSM - ausgeführt werden, wo sie vor Angriffen geschützt sind, die auf standardmäßigen serverbasierten Plattformen vorherrschen. Qube nutzte CodeSafe für alle Schlüsselhandhabungs- und Ver-/Entschlüsselungsvorgänge und konnte so das höchstmögliche Maß an Sicherheit gewährleisten.
- **Zuverlässigkeit und Reputation**. Um das Vertrauen der Studios und Filmindustrie zu gewinnen, musste Qube die verlässlichsten und glaubwürdigsten Sicherheitslösungen einsetzen, die höchste Anforderungen erfüllen können. Aufgrund bewährter Leistung, manipulationssicherer Hardware und FIPS 140-2 Level 3 zertifiziertem Schutz für kryptographische Schlüssel sind die Entrust nShield HSMs perfekt geeignet.
- **Belastbarkeit und Verfügbarkeit**. Entrust nShield HSMs ermöglichen es Qube, die Verfügbarkeit von Schlüsseln für Vertriebspartner zu gewährleisten – ein entscheidender Aspekt, um Vertrauen in dieser Dienstleistungsbranche aufzubauen. Mit Entrust nShield HSMs, die an mehreren geografischen Standorten ausgeführt werden,

Qube Cinema

WICHTIGSTE VORTEILE

- Überwindung von Sicherheitsschwachstellen von Anwendungen auf Hostseite, indem diese innerhalb einer vertrauenswürdigen Umgebung ausgeführt werden
- Schutz kritischer Anwendungen vor Manipulation, Malware und Trojanern
- Bereitstellung von HSM-Kryptographiediensten zur Unterstützung einer Vielzahl von Verbindungsgeräten
- Zertifizierter Schutz mit nach FIPS 140-2 Level 3 zugelassener manipulationssicherer Hardware
- Reduzierung der Kosten für wichtige Verwaltungsaufgaben

um Belastbarkeit zu gewährleisten, kann Qube einfach Schlüssel sichern und mehrere HSMs synchron halten, um Schlüssel für globale Benutzer bereitzustellen.

- **Skalierbarkeit**. Entrust nShield HSMs ermöglichen Qube die Ausgabe und Verwaltung einer unbegrenzten Anzahl von Schlüsseln, was entscheidend für das potenzielle Wachstum des Online-Dienstes ist, den Qube Digitalkinobetreibern anbietet.
- **Serviceniveau**. Qube war von dem Niveau des Service und Supports seitens Entrust sowohl vor als auch nach dem Kauf sehr beeindruckt.

ÜBER ENTRUST

Entrust ermöglicht vertrauenswürdige Identitäten und Zahlungen sowie verlässlichen Datenschutz und hält damit die Welt sicher in Bewegung. Ein nahtloses und sicheres Umfeld ist heute mehr denn je unerlässlich, sei es bei Grenzübertritten, beim Einkaufen, beim Zugriff auf E-Government-Dienste oder beim Einloggen in Unternehmensnetzwerke. Entrust bietet für genau diese Interaktionen eine unübertroffene Bandbreite an Lösungen für digitale Sicherheit und die Ausstellung von Berechtigungsnachweisen. Mit 2.500 Mitarbeitern und einem weltweiten Partnernetzwerk ist Entrust für Kunden in über 150 Ländern tätig, die sich bei ihren sensibelsten Operationen auf uns verlassen.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com