



ENTRUST



Qube Cinema revoluciona la distribución de cine digital con la ayuda de HSMs nShield de Entrust

KeySmith

QUBE

Cómo un fabricante de tecnología de cine digital acaparó el mercado de la gestión de claves en línea para la distribución de cine digital, al proporcionar los niveles más altos de protección de contenido confiable.

Como fabricante de servidores, proyectores, tecnología de masterización y distribución para cine digital, Qube Cinema vio una oportunidad única para introducir una tecnología altamente disruptiva en el mercado, al tiempo que la industria cinematográfica completaba una transición de una década de la distribución física a la digital. La tecnología digital ofrecía enormes beneficios: era mucho menos costoso producir y enviar discos duros que varios rollos de copias de películas. Las películas digitales podrían distribuirse mucho más rápidamente, lo que permitiría a los distribuidores satisfacer mejor la demanda. Las películas digitales no se degradarían con el tiempo y podrían ser proyectadas por mano de obra menos calificada.

El mayor obstáculo y la razón por la que la industria cinematográfica se quedó atrás de otras industrias en la conversión de analógico a digital, fue la seguridad. Los propietarios del contenido (las empresas que producen películas) estaban increíblemente preocupados por la piratería y querían medidas de seguridad increíblemente altas. Los propietarios y distribuidores de cines, por otro lado, no querían tener que lidiar con medidas de seguridad complicadas o costosas que dañaran la rentabilidad e introdujeran una carga operativa. El equipo de Qube sabía que si podía encontrar una manera eficiente de gestionar las claves de cine digital en línea con el más alto grado de seguridad y que también fuera notablemente fácil de operar, sería capaz de revolucionar la industria.

APRENDA MÁS EN [ENTRUST.COM/HSM](https://www.entrust.com/hsm)



LA SOLUCIÓN: KEYSMITH: UN SISTEMA DE ADMINISTRACIÓN DE CLAVES EN LÍNEA POTENCIADO POR HSMs NSHIELD DE ENTRUST

Para abordar la necesidad de una seguridad eficiente en la distribución de cine digital, Qube utilizó módulos de seguridad de hardware (HSMs) nShield® de Entrust para desarrollar un sistema de distribución fácil de usar con el nivel de seguridad más sólido disponible en la industria. En el cine digital, las películas se codifican y cifran en un paquete de cine digital (DCP) y se distribuyen a través del disco duro o la señal satelital, luego se pueden descifrar en el cine con la información contenida en un mensaje de entrega de claves (KDM) único que desbloquea la película para un teatro específico, un calendario y un número de funciones.

KeySmith satisface los requisitos de propietarios y distribuidores de contenido por igual. Los propietarios de contenido ya no tienen que preocuparse por las medidas de cifrado internas basadas en software que suelen utilizar los distribuidores, o en el peor de los casos: perder las claves de cifrado y quedar bloqueado de su propio contenido. Los HSMs nShield de Entrust ofrecen el grado más alto de protección para las claves de cifrado de contenido en la industria, al mismo tiempo que garantizan que las claves nunca se pierdan. Para los distribuidores y propietarios de salas de cine, el sistema Qube también proporciona un nivel de facilidad operativa que elimina cualquier barrera para implementar una alta seguridad o la tentación de sacrificar la seguridad en aras de la conveniencia.

Así es como funciona el sistema: un estudio o un cineasta independiente envía una película para su distribución. Se convierte a DCP, que es un formato estándar de la industria para los archivos multimedia y los metadatos que componen una película. Dentro del DCP, se utiliza un conjunto de claves AES para cifrar archivos individuales. Un KDM de distribución (DKDM) que lleva estas claves de forma segura, se pone a disposición de la cuenta

de KeySmith del distribuidor. Este DKDM le permite a KeySmith generar KDMs para teatros individuales. Los HSMs nShield de Entrust crean un par de claves pública/privada RSA únicas y un certificado digital asociado para cada empresa dentro de KeySmith. Estos HSMs cifran las claves AES con la clave pública del teatro receptor mediante una aplicación que se ejecuta dentro del límite de seguridad certificado del HSM. Solo el destinatario previsto puede descifrar el paquete con la clave privada asociada, que es única y está instalada de forma segura en el momento de la fabricación. KeySmith también puede entregar los KDM directamente a los cines. Por lo general, esto se lleva a cabo después de que los cines reciben la película a través del disco duro o la descarga vía satélite. Es un sistema altamente eficiente que proporciona facilidad de uso para los distribuidores y, al mismo tiempo, garantiza una protección de alta seguridad del contenido de la película, dos elementos críticos de la propuesta de valor comercial de Qube.

ACERCA DE LA SOLUCIÓN

Los HSMs nShield de Entrust proporcionan un entorno reforzado y resistente a manipulaciones indebidas para realizar un procesamiento criptográfico seguro, la protección y administración de claves. Con estos dispositivos puede implementar soluciones de alta seguridad que cumplen con los estándares establecidos y emergentes de cuidado debido para los sistemas criptográficos y las prácticas recomendadas, mientras que también mantiene altos niveles de eficiencia operacional.

Los HSMs nShield de Entrust están certificados por autoridades independientes, lo que establece puntos de referencia de seguridad cuantificables que le brindan confianza en su capacidad para respaldar los mandatos de cumplimiento y las políticas internas. Los HSMs nShield de Entrust están disponibles en varios factores de forma para admitir todos los escenarios



de implementación comunes, desde dispositivos portátiles hasta dispositivos de centro de datos de alto rendimiento.

Con los HSMs nShield de Entrust usted puede:

- Ofrecer protección certificada para claves criptográficas y operaciones en un hardware a prueba de manipulaciones indebidas para mejorar la seguridad para aplicaciones críticas.
- Conseguir una aceleración criptográfica rentable y una flexibilidad operacional inigualable en centros de datos y entornos en la nube tradicionales.
- Superar las vulnerabilidades de seguridad y los retos de rendimiento de la criptografía de software.
- Reducir el coste de cumplimiento con la normativa y las tareas cotidianas de gestión de claves que incluyen las copias de seguridad y la gestión remota. Con los HSMs nShield de Entrust, puede comprar la capacidad que necesite y escalar su solución de forma fácil y a medida que sus necesidades cambien.

ENTRUST CODESAFE

El kit de herramientas para desarrolladores CodeSafe proporciona la capacidad única para mover aplicaciones confidenciales dentro del perímetro protegido de un HSM nShield certificado. Cargadas y ejecutadas de forma segura en HSMs FIPS 140-2 de nivel 3, las aplicaciones están protegidas contra la manipulación indebida y pueden descifrar, procesar y cifrar datos dentro de este entorno seguro.

CodeSafe permite que las organizaciones:

- Prevengan el robo de propiedad intelectual proporcionando control remoto de aplicaciones sensibles sin importar el entorno, y ofreciendo servicios criptográficos independientemente del sistema operativo o la configuración utilizada por

el cliente, ya sea servidor o computador central. CodeSafe también les permite a los propietarios de aplicaciones o dispositivos portátiles mantener un entorno de ejecución de aplicaciones actualizado sin presencia física.

- **Proteja las aplicaciones de ataques** por parte de hackers o administradores deshonestos al brindar la capacidad de firmar digitalmente aplicaciones confiables para que se verifique su integridad antes de su lanzamiento. CodeSafe también protege las aplicaciones contra el robo, incluso en entornos no controlados que utilizan la subcontratación y la contratación.
- **Proteja los datos confidenciales de SSL** proporcionando un verdadero cifrado SSL de un extremo a otro, terminando SSL y procesando los datos confidenciales dentro del HSM para protegerlos de los ataques.

¿POR QUÉ ENTRUST?

La decisión de Qube de utilizar Entrust se vio bajo la influencia de varios factores importantes:

- **CodeSafe.** Los HSMs nShield de Entrust proporcionan una función de seguridad que ninguna otra solución ofrece: CodeSafe permite que las aplicaciones se ejecuten en un entorno seguro, dentro del HSM, donde se hallan protegidas de los ataques que prevalecen en las plataformas estándar basadas en servidores. Qube utilizó CodeSafe para realizar todas las operaciones de manejo de claves y cifrado/descifrado, proporcionando el mayor nivel de seguridad posible.
- **Fiabilidad y reputación.** Qube sabía que para ganarse la confianza de los estudios y la industria cinematográfica, necesitaría elegir las soluciones de seguridad más confiables y creíbles que resistieran los más altos niveles de escrutinio.



VENTAJAS PRINCIPALES

- Superar las vulnerabilidades de seguridad de las aplicaciones del lado del host, ejecutándolas dentro de un entorno confiable
- Proteger las aplicaciones críticas de la manipulación indebida, el malware y los troyanos
- Poner a disposición los servicios criptográficos del HSM para admitir una amplia variedad de dispositivos de conexión
- Ofrecer protección certificada con hardware resistente a manipulaciones aprobado por FIPS 140-2 Nivel 3
- Reducir el costo de las tareas de gestión de claves

Con un rendimiento comprobado, hardware a prueba de manipulaciones indebidas y protección certificada FIPS 140-2 Nivel 3 para claves criptográficas, los HSMs nShield de Entrust encajan perfectamente.

- **Resistencia y disponibilidad.** Los HSMs nShield de Entrust le permiten a Qube garantizar la disponibilidad de claves para los distribuidores, un aspecto fundamental para generar confianza en esta industria de servicios. Con los HSMs nShield de Entrust ejecutándose en múltiples ubicaciones geográficas para garantizar la resistencia, Qube puede realizar fácilmente copias de seguridad de claves y mantener múltiples HSMs sincronizados para entregar claves a usuarios globales.

- **Escalabilidad.** Los HSMs nShield de Entrust permiten que Qube emita y gestione un número ilimitado de claves, lo que es fundamental para el crecimiento potencial del servicio en línea que Qube ofrece a los proveedores de cine digital.
- **Sensibilidad.** Qube quedó impresionado con el nivel de servicio pre y posventa y soporte que recibió de Entrust.

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Hoy más que nunca, las personas exigen experiencias seguras y sin problemas, ya sea que crucen fronteras, realicen una compra, accedan a servicios de gobierno electrónico o inicien sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.



Aprenda más en

entrust.com/HSM



ENTRUST