Fastcom incrementa la eficiencia de la firma de código al mismo tiempo que mantiene altos niveles de seguridad

www.fastcom-technology.com

EL DESAFÍO: UN MEJOR DECODIFICADOR PARA AYUDAR A FOXTEL A MANTENER SU VENTAJA COMPETITIVA

El mercado de la televisión de paga es muy competitivo, y los consumidores exigen regularmente accesos a nuevas ofertas de contenido. Incluso en Australia, donde Foxtel lidera el mercado de la televisión de paga, el ingreso al mercado por parte de nuevos operadores significa que Foxtel debe mantenerse aún más enfocado en las nuevas innovaciones para continuar brindando una excelente experiencia al suscriptor.

Foxtel presentó el decodificador (STB) iQ3, que ofrece flujos de contenido mejorados, más espacio de grabación y características nuevas adicionales destinadas a aumentar la satisfacción de los suscriptores.

Al diseñar el iQ3, Foxtel se comprometió con Fastcom e identificó tres requisitos básicos. Específicamente, los decodificadores necesitaban:

- Apoyar una estrategia de seguridad de múltiples proveedores, lo cual le permite a Foxtel la flexibilidad para ofrecer transmisiones desde múltiples proveedores de contenido, así como también cambiar proveedores según sea necesario.
- Evita el acceso no autorizado al contenido solo por suscripción
- Proporciona a Foxtel control directo sobre los dispositivos implementados para permitir actualizaciones eficientes que respondan a las necesidades del cliente.

LA SOLUCIÓN: MCAS DE FASTCOM, HABILITADO POR ENTRUST

Basándose en las necesidades de Foxtel, Fastcom desarrolló las especificaciones iniciales para su solución de sistema de acceso condicional múltiple (MCAS), determinando rápidamente que requeriría de criptografía altamente segura, comenzando con la fabricación de los decodificadores. De hecho, la clave raíz que proporciona una raíz de confianza para todo el cifrado y descifrado en el dispositivo debería grabarse en los procesadores centrales del iQ3, estableciendo la identidad de cada dispositivo y permitiendo la creación de claves para cifrar el contenido del sistema de acceso condicional (CAS)/soluciones de gestión de derechos digitales (DRM).

APRENDA MÁS EN ENTRUST.COM/HSM

Fastcom

Para lograr el nivel de seguridad exigido por la aplicación, Fastcom determinó que necesitaban ejecutar su algoritmo de derivación de claves dentro de un entorno certificado por FIPS. Fastcom estaba familiarizado con los módulos de seguridad de hardware (HSMs) y estaba seguro de que ofrecían la seguridad y modularidad necesarias.

Después de revisar varias ofertas de proveedores, Fastcom seleccionó los HSMs nShield® de Entrust debido a su capacidad incomparable para cumplir con todos los requisitos de seguridad del proyecto. Específicamente, nShield CodeSafe presenta una capacidad inigualable que le permite a Fastcom ejecutar su algoritmo de derivación patentado y proteger claves dentro de un límite de nivel 3 de FIPS 140-2.

Durante la fase de implementación, el equipo de Entrust desarrolló parte del código de la aplicación de cifrado dentro del entorno CodeSafe, que Fastcom luego modificó. Esto le proporcionó a Fastcom la ventaja que necesitaba para desarrollar la solución y, al mismo tiempo, le permitió asumir fácilmente la propiedad del código central.

Usando el HSM nShield, Fastcom deriva múltiples claves subordinadas de una sola clave raíz para que Foxtel las incorpore en los decodificadores iQ3. Los proveedores de CAS utilizan las claves para cifrar el contenido que llega a través de las soluciones CAS/DRM, lo cual garantiza que el contenido solo se pueda reproducir en un decodificador en particular.

Con el respaldo que los HSMs nShield de Entrust le dan a la solución MCAS, Foxtel puede elegir libremente las aplicaciones, middleware y soluciones CAS/DRM para sus decodificadores iQ3. Esto permite un enfoque de múltiples proveedores, así como actualizaciones eficientes y de bajo costo para los decodificadores según sea necesario, y la entrega de contenido premium a los suscriptores de televisión por pago. De cara al futuro, Fastcom prevé utilizar el modelo MCAS para desarrollar otras soluciones de equipos en las instalaciones del cliente que aprovechen su enfoque de seguridad de múltiples proveedores.

VENTAJAS PRINCIPALES

- Cambie fácilmente los proveedores de CAS y el middleware sin actualizaciones costosas a los decodificadores
- Obtenga control directo sobre los dispositivos implementados de forma remota, mejorando la experiencia del suscriptor
- Proteja las fuentes de ingresos asegurando contenido premium

ACERCA DE LA SOLUCIÓN

HSMs nShield de Entrust

Los HSMs nShield de Entrust proporcionan un entorno reforzado y resistente a las manipulaciones indebidas para realizar un procesamiento criptográfico seguro, la protección y gestión 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.

Fastcom

CODESAFE DE ENTRUST

El kit de herramientas para desarrolladores Entrust CodeSafe proporciona la capacidad única para mover aplicaciones confidenciales dentro del perímetro protegido de un HSM nShield certificado FIPS 140-2 Nivel 3. Con este enfoque, las aplicaciones están protegidas de las manipulaciones indebidas y pueden descifrar, procesar y cifrar datos dentro del entorno seguro.

CODESAFE PERMITE QUE LAS ORGANIZACIONES:

- **Prevenga 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.

ACERCA DE FASTCOM

Fastcom, una empresa suiza independiente, ofrece soluciones de seguridad y consultoría técnica al mercado de la televisión de paga.

La solución MCAS de Fastcom es un conjunto integrado de servicios de autorización de licencias para equipos en las instalaciones del cliente tales como decodificadores de televisión por pago (STB). Tomando provecho de una infraestructura modular y escalable, el MCAS admite simultáneamente múltiples sistemas de acceso condicional (CAS) y soluciones de administración de derechos digitales (DRM), al tiempo que brinda a los operadores de televisión por pago control directo de los decodificadores en el campo.

ACERCA DE FOXTEL

Foxtel es la principal empresa de medios de Australia y ofrece servicios de Internet y televisión de paga a más de 2,8 millones de hogares en todo el país.

ACERCA DE ENTRUST

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Ahora más que nunca, la gente necesita experiencias seguras impecables, mientras cruzan fronteras, realizan compras, acceden digitalmente a servicios del gobierno o inician 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 de más de 150 países, no es una sorpresa que la mayoría de organizaciones autorizadas del mundo confíen en nosotros.

Fastcom

CON LOS HSMS NSHIELD DE ENTRUST USTED PUEDE:

- Ofrecer protección certificada para claves criptográficas y operaciones en un hardware a prueba de manipulaciones para mejorar la seguridad para aplicaciones críticas
- Conseguir una aceleración criptográfica rentable y una flexibilidad operacional inigualable en centros de datos tradicionales y entornos en la nube
- 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.

¿POR QUÉ ENTRUST?

- Entrust ganó el negocio según en la seguridad y la funcionalidad única de los HSMs nShield, respaldado por la experiencia en implementación de Entrust.

Entrust le ofreció a Fastcom:

- Seguridad líder en la industria. Fastcom sabía que necesitaba ofrecer una solución en la que Foxtel pudiera confiar para proteger el contenido premium del acceso no autorizado una vez que se implementaron los decodificadores iQ3 en el campo. Con los HSM nShield de Entrust en su núcleo, la solución MCAS ofrece los más altos niveles de seguridad y funcionalidad
- Un entorno protegido para ejecutar su algoritmo criptográfico. Fastcom había desarrollado su propio algoritmo de derivación de claves para el que quería el nivel más alto de protección disponible. Entrust CodeSafe es la única solución que permite que las aplicaciones se ejecuten dentro de los límites certificados por FIPS del HSM, donde están protegidas de los ataques que prevalecen en las plataformas estándar basadas en servidores.
- Experiencia en seguridad altamente calificada. Los expertos del equipo de servicios profesionales de Entrust colaboraron con Fastcom para comenzar a construir la aplicación que derivaría las claves de raíz de confianza que protegen los decodificadores iQ3. Fastcom aprovechó este salto inicial para acelerar el desarrollo de la solución MCAS

mcas

Aprenda más en
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com