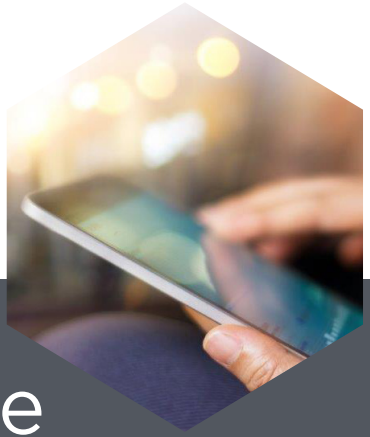
Módulos de Seguridad de Hardware (HSMs) de Uso General nShield®

ENTRUST

SECURING A WORLD IN MOTION

Índice



Seguridad en la que puede confiar

Los módulos de seguridad de hardware (HSMs) nShield de Entrust son dispositivos reforzados y resistentes a manipulaciones indebidas que protegen los datos más confidenciales de su empresa. Estos módulos con certificación FIPS 140-2 realizan funciones criptográficas como la generación, administración y almacenamiento de claves codificadas y firmadas, así como la ejecución de las funciones sensibles dentro de sus límites protegidos.

Una adición poderosa a su portafolio de seguridad, los HSM nShield le ayudan a:

- Lograr altos niveles de seguridad y confianza de datos
- Cumplir y superar los estándares regulatorios más importantes
- Mantener altos niveles de servicio y agilidad empresarial

La familia de productos nShield

Para encajar con su entorno específico, la familia de productos de HSM nShield para uso general incluye los siguientes modelos:

nShield Connect

Dispositivos conectados a la red

Los HSM nShield Connect proporcionan servicios criptográficos a aplicaciones distribuidas a través de la red. Los HSMs nShield Connect están disponibles en dos series: HSM nShield Connect+ clásicos y la serie HSM nShield Connect XC de alto rendimiento.

nShield Edge

Módulo portatil con conexión USB

Los HSMs nShield Edge son dispositivos de escritorio diseñados para su comodidad y economía. El módulo nShield Edge es ideal para desarrolladores y apoya aplicaciones de bajo volumen tales como la generación de claves de raíz.

nShield Solo

Tarjetas PCIe para integrar en dispositivos o servidores

Los HSM nShield Solo son módulos de tarjetas PCI-Express de bajo perfil que proporcionan servicios criptográficos a las aplicaciones alojadas en un servidor o dispositivo. Los HSM nShield Solo están disponibles en dos series: HSM nShield Solo+ clásicos y la serie HSM nShield Solo XC de alto rendimiento.

nShield as a Service

Solución por suscripción para acceder a HSM nShield en la nube

nShield as a Service proporciona acceso a HSM nShield Connect XC con certificación FIPS 140-2 de nivel 3 a través de un modelo de suscripción. La solución ofrece las mismas prestaciones y funcionalidad que los HSM instalados en las instalaciones y las ventajas del uso de un servicio en la nube. Esto permite que los clientes cumplan sus principales objetivos en la nube y dejen el mantenimiento de estos dispositivos en manos de los expertos de Entrust. Disponible como opciones de servicio autogestionado y totalmente gestionados.

Compatible con una amplia variedad de usos

Los clientes de Entrust usan los HSM nShield como su fuente de confianza en diversas aplicaciones comerciales, entre ellas las PKI, la protección de claves de cifrado SSL/TLS, la firma de códigos, la firma digital y blockchain. Con el crecimiento del Internet de las Cosas se genera mayor demanda de identificación de dispositivos y certificados, los HSMs nShield continuarán brindando apoyo para las medidas de seguridad críticas, tales como la autenticación de dispositivos que usan certificados digitales.

Los HSM nShield también apoyan una amplia gama de algoritmos criptográficos, incluidos los algoritmos criptográficos de curva elíptica que permiten realizar transacciones de alta velocidad adaptadas a los entornos informáticos compactos actuales, así como sistemas operativos más extensamente utilizados del sector y API

Funcionalidades de la familia de productos nShield

Interfaces de servicios web compatible con la nube

El paquete Web Services Option Pack de nShield optimiza la interfaz entre sus aplicaciones y HSM al ejecutar comandos a través de llamadas de servicio web. Este enfoque innovador facilita las implementaciones y quita la necesidad de depender del diseño de la arquitectura y el sistema operativo elegido. Una solución compatible con la nube, el paquete de opción de servicios web se intercomunica con aplicaciones alojadas en la nube, así como en los centros de datos tradicionales.

Soporte contenerizado en instalaciones o en la nube

El nShield Container Option Pack permite el desarrollo y la implementación impecable de aplicaciones contenidas o procesos respaldados por los módulos de seguridad de hardware de Entrust altamente garantizados. Esta opción proporciona un conjunto de scripts preempaquetados que simplifican en gran medida la integración de los HSM nShield en un entorno de aplicación de contenedor a la vez que soporta las necesidades dinámicas y de escalamiento de las aplicaciones y los servidores contenidos de los clientes.

Administración de claves más sólida para sus datos en la nube con nShield BYOK

nShield BYOK (Bring Your Own Key) le permite generar claves robustas en el HSM nShield ubicado en las instalaciones y exportarlas de forma segura a sus aplicaciones en la nube, ya sea si utiliza Amazon Web Services, Google Cloud Platform, Microsoft Azure, o las tres. Con nShield BYOK, fortalece la seguridad de sus prácticas de administración de claves, obtiene un mayor control de sus claves y garantiza que está compartiendo la responsabilidad de mantener sus datos seguros en la nube.

nShield BYOK ofrece las siguientes ventajas:

- Prácticas de administración de claves más seguras que fortalecen la seguridad de sus datos confidenciales en la nube.
- Generación de claves más robustas al utilizar el generador de números aleatorios de alta entropía de nShield protegido por hardware certificado en conformidad con la norma FIPS
- Más control sobre sus claves, utilice sus propios HSM nShield en su propio entorno para crear, almacenar y exportar de forma segura sus claves en la nube

Para una mayor seguridad y controles estrictos sobre el transporte y el uso de claves criptográficas utilice nCipher BYOK con Microsoft Azure. Si necesita asistencia en las instalaciones con la integración e implementación, por qué no elegir nuestro paquete de servicio de implementación BYOK. Este paquete incluye un nShield Edge, integración por parte del equipo de servicios profesionales de Entrust y un año de mantenimiento.

Para BYOK en Amazon Web Services y Google Cloud Platform, elija el paquete de opción de integración en la nube (Cloud Integration Option Pack, CIOP). El paquete opcional contiene todo lo que necesita para usar HSM nShield de forma local para generar y asignar sus claves a Amazon Web Services o Google Cloud Platform. Además, CIOP ofrece soporte para el nuevo mecanismo Microsoft Azure BYOK de plataforma abierta.

Optimización de operaciones utilizando administración y monitoreo de manera remota

nShield Monitor y nShield Remote Administration, disponibles para los HSM nShield Solo y Connect, le ayudan a reducir los costos operativos a la vez que se mantiene informado y en control 24x7 de
sus estados de HSM.

- La supervisión y administración remota de Entrust ofrece las siguientes ventajas:
- Optimiza el rendimiento, la planificación de la infraestructura y tiempo de actividad de HSM utilizando nShield Monitor para informar a su personal sobre las tendencias de carga, estadísticas de uso, eventos de falsificación, advertencias y alertas
- Reducir los gastos en viáticos y ahorrar tiempo al administrar los HSMs a través de la interfaz robusta y segura de nShield Remote Administration

Configuración remota

Los modelos nShield Connect XC ofrecen una opción de consola en serie simplificando la instalación física del HSM para alinear, cablear y aplicar potencia. La configuración de todos los otros HSM y red se puede realizar de forma remota. Esto facilita la implementación y la reimplementación sin necesidad de revisitar el centro de datos. Esta prestación soporta un modelo de proveedor/usuario mientras que el proveedor controla la configuración de red y el usuario tiene pleno control de su material de claves.

Arquitectura altamente flexible de Security World

La arquitectura de Security World de nShield admite HSM nShield de Entrust mediante la creación de un entorno de administración de claves flexible y exclusivo. Con Security World de nShield, usted puede combinar diferentes modelos de HSM nShield para construir un ecosistema unificado que ofrece escalabilidad, perfecta tolerancia a fallos y balance de carga.

"Los HSM nShield de Entrust son innovadores y nos han permitido utilizar un chip más sofisticado y seguro en nuestra tecnología."

Bill Kavadas, Director Senior para Sistemas de Información, Memjet

nShield Security World proporciona interoperatividad tanto si implementa uno o cientos de HSM, le permite gestionar un número ilimitado de claves y copia y restaura el material de claves de forma automática y remota.

nShield Security World ofrece las siguientes ventajas:

- Le ayuda a escalar de forma fácil su estado de HSM nShield a medida que sus necesidades crecen
- Conserva la resistencia del sistema
- Ahorra tiempo eliminando las copias de seguridad de los HSM que llevan tanto tiempo

CodeSafe - el entorno de ejecución segura de nShield

Además de proteger sus claves confidenciales, los HSM nShield Solo y Connect no solo protegen sus claves y datos confidenciales; también proporcionan un entorno seguro para ejecutar sus aplicaciones propias. La opción CodeSafe le permite desarrollar y ejecutar el código dentro de los límites FIPS 140-2 de nivel 3 de nShield, protegiendo sus aplicaciones de posibles ataques.

CodeSafe le ayuda a:

- Lograr una alta garantía al ejecutar aplicaciones sensibles y proteger los criterios de valoración de datos de aplicación dentro de un entorno certificado
- Proteger las aplicaciones que requieren seguridad contra riesgos, tales como los ataques de agentes internos, el malware y las amenazas persistentes avanzadas
- Eliminar el riesgo de cambios de aplicación no autorizados o la infección de malware utilizando la firma de códigos

Alianzas con líderes de la industria

Entrust tiene alianzas con proveedores de servicios tecnológicos líderes en la industria para ofrecer soluciones mejoradas que abordan un amplio conjunto de desafíos de seguridad del sector y ayudan a los clientes a lograr sus objetivos de transformación digital. A través del programa de asociación tecnológica de Entrust, Entrust través del programa de sus socios tecnológicos, colabora para integrar HSM nShield en una variedad de soluciones de seguridad incluyendo la creación de credenciales y PKI, seguridad de base de datos, firma de códigos, firmas administración, gestión de cuentas privilegiadas, entrega de aplicaciones, inteligencia en la nube y los big data. Los HSM nShield son compatibles con las aplicaciones de seguridad de nuestros socios para ofrecer el procesamiento criptográfico más sólido, la protección de claves y la administración de claves disponibles, a la vez que se facilita el cumplimiento de las normativas de en materia de seguridad de datos del gobierno y la industria.

"Nos emocionan las posibilidades que las nuevas prestaciones compatibles con la nube de nShield, incluido nShield as a Service, ofrece a nuestros clientes. Estas nuevas prestaciones reconocen que el mercado está cambiando; que la organización necesita la capacidad de HSM integral en la nube para liberar la innovación y las ventajas comerciales disponibles."

Ed Wood, Director de Gestión de Producto, Cryptomathic

"El lanzamiento de nShield as a Service de Entrust proporciona a los clientes F5 opciones de seguridad mejoradas con la capacidad de lograr la soberanía de datos en un modelo basado en la suscripción. Cambiar la seguridad de un capital a un gasto operativo permite una mayor flexibilidad y rentabilidad para las organizaciones".

John Morgan, Vicepresidente y Gerente General de Seguridad, redes F5

Versatilidad y alto rendimiento

Los HSM nShield Connect y Solo están disponibles en tres niveles de rendimiento para adaptarse a su entorno, ya sea que sus índices de transacción sean moderados o que su aplicación exija un alto rendimiento. nShield as a Service, nuestra solución basada en suscripción para acceder a los HSM nShield en la nube está respaldada por nuestro nShield de mayor rendimiento, el Connect XC.

Certificación con los estándares de la industria

Gracias a que Entrust se adhiere a estándares rigurosos, usted puede a demostrar el cumplimiento en entornos regulados mientras ofrece altas garantías en la seguridad e integridad de los HSM nShield. A continuación, incluimos una lista parcial de los estándares que cumplimos. Las listas completas están disponibles en nuestra página web y en nuestras hojas de información.

FIPS 140-2

FIPS 140-2 es un estándar reconocido mundialmente del Instituto Nacional de Estándares y Tecnología (NIST), una entidad pública de EE. UU. que valida la solidez de la seguridad de los módulos de cifrado. Todos los HSM nShield de Entrust tienen la certificación FIPS 140-2 de nivel 2 y 3.

FIPS Level 3 Validated 140-2

Common Criteria

Cumplimiento con Common Criteria y eIDAS

Los HSM nShield XC y nShield + tienen la certificación Common Criteria EAL4+ y están reconocidos como dispositivos de creación de firmas cualificados (QSCD) bajo la normativa eIDAS. Además, los HSM nShield Solo XC y Connect XC cumplen con el perfil de protección de criterios comunes EN 419 221-5 "Módulos criptográficos para servicios de confianza". Los HSM nShield pueden servir como estructura de seguridad para la digitalización de los estados miembros y empresas de la UE. Esto incluye los programas de identificación nacional y los servicios fronterizos, servicios para la firma de documentos electrónicos y transacciones, además de servicios para la autenticación, impresión temporal, correo electrónico seguro, y conservación de documentos a largo plazo. Aunque estas certificaciones fueron establecidas como parte de una normativa europea, están siendo adoptadas en muchos países.

Para más información

Visítenos en **entrust.com/HSM** para saber cómo podemos proteger su información y aplicaciones esenciales empresariales, en sus propias instalaciones, en la nube y en entornos virtuales.

Para saber más sobre los HSM nShield de Entrust

HSMinfo@entrust.com
entrust.com/HSM

SOBRE ENTRUST CORPORATION

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.

Más información
entrust.com/HSM

ENTRUST

Contáctenos:
HSMinfo@entrust.com