nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

Módulos de Seguridad de Hardware (HSMs) de propósito general nShield®

Índice

Seguridad en la que puede confiar

Los Módulos de Seguridad de Hardware (HSMs) nShield de nCipher son dispositivos reforzados a prueba de manipulaciones indebidas que protegen los datos más confidenciales de su empresa. Estos módulos con certificación FIPS 140-2 realizan funciones de criptografía, tales como generar, administrar y almacenar llaves de firma y cifrado y también ejecutan códigos sensibles dentro de sus límites protegidos.

Los HSM nShield, un complemento poderoso para su pila de seguridad, lo ayudan a:

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

La familia de productos nShield

La familia nShield de HSM para propósitos generales incluye los siguientes modelos para adaptarse a su entorno específico:

NSHIELD CONNECT

Dispositivos conectados a redes

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

NSHIELD EDGE

Módulos portátiles con conexión USB

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

NSHIELD SOLO

Tarjetas PCIe para integrar en dispositivos o servidores

Los HSMs nShield Solo son módulos en formato de tarjetas PCI-Express de bajo perfil que proporcionan servicios criptográficos a aplicaciones alojadas en servidores donde son instaladas. Los HSMs nShield Solo están disponibles en dos series: el clásico HSM nShield Solo+ y el HSM nShield Solo XC de alto rendimiento.

NSHIELD AS A SERVICE

Solución basada en suscripción para acceder a los HSMs nShield desde la nube

nShield as a Service proporciona acceso a los HSMs nShield Connect XC exclusivos con certificación FIPS 140-2 Nivel 3 a través de un modelo de suscripción. La solución ofrece las mismas características y funcionalidades que los HSMs locales, combinados con los beneficios de una implementación de servicios en la nube. Esto les permite a los clientes cumplir con sus primeros objetivos en la nube y dejar el mantenimiento de estos dispositivos a los expertos de nCipher. Disponible como opciones de servicio autogestionadas y totalmente administradas.

Compatible para un amplio rango de usos

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

Los HSMs nShield también apoyan una amplia gama de algoritmos criptográficos, incluidos los algoritmos de criptografía de curva elíptica que permiten realizar transacciones de alta velocidad adaptadas perfectamente a los entornos informáticos compactos de hoy en día, así como a los sistemas operativos y las APIs más utilizadas de la industria.

Funcionalidades de la familia de productos nShield

INTERFACES DE SERVICIOS WEB COMPATIBLES PARA LA NUBE

El nShield Web Services Option Pack, disponible de manera opcional, optimiza la interfaz entre sus aplicaciones y los HSMs ejecutando comandos a través de llamadas de servicios web. Este enfoque innovador simplifica las implementaciones al eliminar la necesidad de integrar aplicaciones directamente con nShield y elimina la necesidad de depender del diseño de la arquitectura y el sistema operativo elegido. nShield Web Services Option Pack, es una interface amigable con la nube que permite interactuar con aplicaciones alojadas en la nube y en centros de datos tradicionales.

SOPORTE EN CONTENEDORES EN LAS INSTALACIONES O EN LA NUBE

El nShield Container Option Pack permite el desarrollo y la implementación sin problemas de aplicaciones o procesos en contenedores, respaldados por los Módulos de Seguridad de Hardware de alta seguridad de nCipher. Esta opción proporciona un conjunto de secuencias de comandos preempaquetadas que simplifican en gran medida la integración de los HSMs nShield en un entorno de aplicación de contenedor, al tiempo que respalda las necesidades dinámicas y de escala de las aplicaciones de los clientes y los hosts en contenedores.

ADMINISTRACIÓN DE LLAVES MÁS SÓLIDA PARA SUS DATOS EN LA NUBE CON NSHIELD BYOK

nShield BYOK (Traiga su propia llave, por sus siglas en inglés) le permite generar llaves mas robustas en el HSM nShield ubicado in situ y exportarlas de forma segura a sus aplicaciones en la nube, ya sea que use Amazon Web Services, Google Cloud Platform, Microsoft Azure, o los tres servicios juntos. Con nShield BYOK, usted fortalece la seguridad de sus prácticas de administración de llaves, logrando mayor control de sus llaves y se cerciora de compartir la responsabilidad de preservar la seguridad de los datos en la nube.

nShield BYOK le ofrece los siguientes beneficios:

- Prácticas de administración de llaves más seguras que fortalecen la seguridad de sus datos confidenciales en la nube.
- Generación de llaves más robustas al utilizar el generador de números aleatorios de alta entropía de nShield, protegido por hardware certificado en conformidad con la norma FIPS
- Mayor control sobre las llaves: use su propio HSM nShield en su propio entorno para crear llaves y exportarlas de forma segura a la nube

Para BYOK en Amazon Web Services y Google Cloud Platform, elija el paquete opcional de nCipher, Cloud Integration Option Pack (CIOP). El paquete opcional contiene todo lo que necesita para usar sus HSM locales de nShield para generar y alquilarle sus llaves a Amazon Web Services o Google Cloud Platform.

Para usar nShield BYOK con Microsoft Azure, elija el paquete de servicio de implementación BYOK de nCipher. Este paquete incluye un nShield Edge, la integración entregada por el equipo de servicios profesionales de nCipher y un año de mantenimiento.

OPERACIONES OPTIMIZADAS SI UTILIZA REMOTE MONITORING Y REMOTE MANAGEMENT

nShield Monitor y nShield Remote Administration, disponibles para los HSMs nShield Solo y Connect, le permiten reducir los costos operativos mientras se mantiene informado y en control del estado de sus HSMs las 24 horas del día, los siete días a la semana.

El monitoreo y la administración remota de nCipher ofrecen los siguientes beneficios:

- Optimizar el rendimiento del HSM, la planificación de la infraestructura y el tiempo de actividad mediante el uso de nShield Monitor para informar a su personal sobre las tendencias de carga, las estadísticas de uso, los casos de manipulación indebida, las advertencias y las 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 que simplifica la instalación física del HSM en estanterías, cableado y suministro de energía. Todas las demás configuraciones de HSM y de red se pueden hacer de forma remota. Esto facilita la implementación y la reasignación sin la necesidad de volver a visitar el centro de datos. Esta característica admite un modelo de proveedor o inquilino, donde el proveedor controla la configuración de la red y el inquilino tiene control total de su material clave.

LA ARQUITECTURA ALTAMENTE FLEXIBLE DE SECURITY WORLD

Los HSMs nShield son una parte integral de la arquitectura de nCipher Security World, que crea un entorno de administración de llaves flexible sin precedentes. Con Security World, usted puede combinar diferentes modelos de HSMs nShield para construir un ecosistema unificado que ofrece escalabilidad, perfecta tolerancia a fallos y balance de carga.

Security World ofrece interoperabilidad ya sea que despliegue uno o cientos de HSMs, le permite administrar un sinnúmero de llaves y crear copias de seguridad y restaurar el material de las llaves en forma automática y remota.

El Security World de nCipher ofrece los siguientes beneficios:

- Lo ayuda a escalar fácilmente el estado de su HSM nShield a medida que sus necesidades van creciendo
- Preserva la resiliencia del sistema
- Ahorra tiempo al eliminar procesos complejos de copias de seguridad de HSM

"Los HSMs nShield de nCipher son de última generación y, por lo tanto, nos han permitido utilizar un chip más sofisticado y seguro en nuestra tecnología."

Bill Kavadas, Director Senior de Sistemas de Información, Memjet

CODESAFE: EL ENTORNO DE EJECUCIÓN SEGURO DE NSHIELD

Además de proteger sus llaves confidenciales, los HSM nShield Solo y Connect también proporcionan un entorno seguro para la ejecución de sus aplicaciones patentadas. La opción CodeSafe le permite desarrollar un código y ejecutarlo dentro de los límites de nShield, que cuenta con la certificación FIPS 140-2 Nivel 3 y así proteger sus aplicaciones de ataques potenciales.

CodeSafe lo ayuda a:

- Lograr una alta seguridad al ejecutar aplicaciones confidenciales y proteger los puntos de conexión de los datos de la 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 que se realicen cambios no autorizados en la aplicación o la infección con malware usando la code signing

Alianzas con líderes de la industria

nCipher tiene alianzas con proveedores de servicios tecnológicos líderes en la industria para brindar soluciones que abordan un amplio conjunto de desafíos de seguridad de la industria y ayudan a los clientes a alcanzar sus objetivos de transformación digital. nCipher, a través del programa de sus socios tecnológicos, colabora con los socios para integrar los HSM nShield en una variedad de soluciones de seguridad que incluyen credenciales e Infraestructura de llave pública (PKI), seguridad de bases de datos, firma de códigos, firmas digitales, administración de cuentas privilegiadas, entrega de aplicaciones e inteligencia en la nube y Big Data. Los HSM nShield son compatibles con las aplicaciones de seguridad de nuestros socios para proporcionar el procesamiento criptográfico más sólido, la protección de llaves y la administración de llaves disponibles, al tiempo que facilita el cumplimiento de las normativas en materia de seguridad de datos del gobierno y la industria.

"El lanzamiento de nShield as a Service de nCipher Security ofrece a los clientes de F5 opciones de seguridad mejoradas, con la capacidad de lograr la soberanía de los datos, en un modelo basado en 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, F5 Networks

"Estamos entusiasmados con las posibilidades que las nuevas funciones amigables con la nube de nShield, incluido nShield as a Service, les ofrecen a nuestros clientes. Estas nuevas características reconocen que el mercado está cambiando; que las organizaciones necesitan las capacidades de los HSMs como servicios completos en la nube, para liberar la innovación y los beneficios comerciales disponibles".

Ed Wood, Director de Gestión de Producto, Cryptomathic

Versatilidad y alto rendimiento

Los HSMs 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 HSMs nShield en la nube está respaldada por nuestro nShield de mayor rendimiento, el Connect XC.

Certificación conforme a los estándares de la industria

Gracias a que nCipher se adhiere a estándares rigurosos, usted puede demostrar su cumplimiento en entornos regulados, al tiempo que brinda un alto grado de confianza en la seguridad y la integridad de los HSMs nShield. A continuación, le ofrecemos 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 HSMs nShield están certificados para FIPS 140-2 Nivel 2 y Nivel 3

CUMPLIMIENTO CON COMMON CRITERIA Y eIDAS

Los HSMs nShield XC y nShield + están certificados según Common Criteria EAL 4+ y reconocidos como dispositivos de creación de firmas calificados (QSCD) según el Reglamento eIDAS. Además, los HSMs nShield Solo XC y Connect XC cumplen con el Perfil de protección de Common Criteria EN 419 221-5 “Cryptographic Modules for Trust Services”. Por lo tanto, los HSMs nShield pueden servir como eje central de la seguridad para la digitalización de los estados miembros y las empresas de la UE. Esto incluye habilitar esquemas de identificación nacional y servicios transfronterizos, servicios para documentos electrónicos y firma de transacciones, además de servicios para autenticación, marca de tiempo, correo electrónico seguro y preservación de documentos a largo plazo. Si bien estas certificaciones se establecieron como parte de un reglamento europeo, están siendo adoptadas por muchos países de todo el mundo.

Para obtener más información

Visítenos en **www.nCipher.com/products/general-purpose-hsms** para conocer cómo podemos proteger la información y las aplicaciones críticas de su negocio, en sus propias instalaciones, en la nube y en entornos virtuales.

nCipher AN ENTRUST DATACARD COMPANY

www.ncipher.com

ACERCA DE NCIPHER SECURITY

nCipher Security, una empresa de Entrust Datacard, lidera el mercado de módulos de Seguridad de Hardware (HSMs) de propósito general y con ello fortalece a las organizaciones líderes en el mundo al brindarles confianza, integridad y control sobre la información y las aplicaciones críticas de sus negocios. El rápido entorno digital de hoy en día mejora la satisfacción del cliente, proporciona una ventaja competitiva y mejora la eficiencia operativa. Y también multiplica los riesgos en seguridad. Nuestras soluciones criptográficas protegen las tecnologías emergentes, tales como la nube, el IoT, el blockchain, los pagos digitales y ayudan a cumplir con las nuevas exigencias en materia de cumplimiento. Esto lo llevamos a cabo utilizando la misma tecnología comprobada de la que dependen las organizaciones globales en la actualidad para protegerse contra las amenazas a sus datos confidenciales, las comunicaciones de red y la infraestructura empresarial. Le ofrecemos confianza para las aplicaciones críticas de su negocio, aseguramos la integridad de sus datos y le damos el control completo , hoy, mañana y en todo momento.
www.ncipher.com

Buscar: nCipherSecurity

CONFIANZA. INTEGRIDAD. CONTROL.