HSM nShield Connect

La seguridad de sus aplicaciones depende de dónde guarda sus claves

PRINCIPALES CARACTERÍSTICAS

Capacidades integrales

Los módulos de seguridad del hardware (HSM) nShield Connect son aplicaciones con certificación FIPS 140-2 y Common Criteria EAL4+ (EN 419 221-5) que ofrecen servicios de claves criptográficas escalables y altamente disponibles entre redes.

- Altas tasas de transacción criptográfica y escalamiento flexible
- Integrar con más de 150 soluciones de proveedores de aplicaciones líderes
- Opción CodeSafe para proteger su aplicación y la lógica empresarial dentro del entorno de ejecución segura de nShield

Los HSM nShield Connect son plataformas resistentes a las falsificaciones que realizan funciones como encriptación, firma digital y la generación y protección de claves para una variedad de aplicaciones, como:

- Autoridades certificadoras
- CodeSafe
- Software personalizado
- La nube y las aplicaciones de contenedores
- Servicios web
- Blockchain
- Cifrado de bases de datos

La serie de nShield Connect incluye a nShield Connect+ y al nuevo nShield Connect XC de alto rendimiento.

APRENDA MÁS EN ENTRUST.COM/HSM

HSM nShield Connect

ASPECTOS CLAVE Y BENEFICIOS

Arquitectura altamente flexible

Nuestra arquitectura única de Security World le permite combinar los modelos HSM nShield para crear un estado combinado que ofrece escalabilidad flexible, migración en caso de falla y equilibrado de carga impecables.

Procesa los datos con mayor rapidez

Los HSM nShield Connect soportan altas tasas de transacción criptográfica, lo que los hace perfectos para entornos donde la capacidad de procesamiento es fundamental, como empresas, comercio minorista e Internet de las cosas.

FUERTES OPCIONES DE CARACTERÍSTICAS REMOTAS

Elimina las visitas al centro de datos

nShield Remote Administration - Permite la presentación remota de manera segura de las tarjetas inteligentes de autorización para que HSM remotos ejecuten tareas de mantenimiento que incluyen actualizaciones de firmware, adicionar nuevos HSM y reasignar/reconfigurar los HSM existentes. Ficha técnica individual disponible.

Configuración remota - La versión de consola de serie Connect XC permite la instalación sencilla para el personal del centro de datos, la configuración de red remota y ajustes del panel frontal.

El nShield Monitor proporciona un panel sencillo de todos sus HSM nShield que le ayuda a optimizar las operaciones y aumenta el tiempo de actividad. Ficha técnica individual disponible.

Proteja sus aplicaciones privadas

La opción CodeSafe proporciona un entorno seguro para ejecutar aplicaciones confidenciales dentro de los límites físicos de nShield FIPS 140-2. Consulte la hoja de datos de CodeSafe para obtener información más detallada.

MODELOS Y RENDIMIENTO DISPONIBLES

Modelos nShield Connect	500+	XC Base	1500+	6000+	XC Medio	XC Alto
Rendimiento de firma RSA (tps) para longitudes de clave recomendadas por NIST						
2048 bits	150	430	450	3000	3500	8600
4096 bits	80	100	190	500	850	2025
Rendimiento de firma de ECC principal (tps) para las longitudes de clave recomendadas NIST						
256 bits	540	680	1260	2400	7515[2]	14 400[2]
Licencias para cliente						
Incluido	3	3	3	3	3	3
Máximo	10	10	20	ilimitado[1]	20	ilimitado[1]

Nota 1: requiere licencia de cliente corporativo.

Nota 2: el rendimiento indicado requiere la activación de la función rápida RNG de ECDSA disponible de forma gratuita a petición del soporte de nCipher.

APRENDA MÁS EN ENTRUST.COM/HSM

HSM nShield Connect

ESPECIFICACIONES TÉCNICAS

Algoritmos criptográficos soportados (incluida la implementación completa de NIST Suite B)

- Algoritmos asimétricos: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (incluyendo NIST, Brainpool y curvas secp256k1), ECDH, Edwards (Ed25519, Ed25519ph)
- Algoritmos simétricos: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, Triple DES
- Resumen de mensajes/algoritmos hash: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bits), HAS-160, RIPEMD160

Plataformas soportadas

- Los sistemas operativos Windows y Linux incluyen la distribución de RedHat, SUSE y los principales proveedores de servicios de la nube que funcionan como máquinas virtuales o en contenedores

Interfaces de programación de aplicaciones (API)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI y CNG, nCore, y Servicios Web (requiere el paquete de opción de servicios Web)

Conectividad de servidor

- Puertos duales Gigabit Ethernet (dos segmentos de red)

Cumplimiento con la seguridad

- Certificación FIPS 140-2 de nivel 2 y 3
- Certificación IPv6 y USGv6 Compatible
- Connect XC: eIDAS y Common Criteria EAL4 + AVA_VAN.5 y certificación ALC_FLR.2 respecto al perfil de protección EN 419 221-5, por el esquema neerlandés NSCIB
- Connect+: certificación Common Criteria EAL4+ (AVA_VAN.5)
- Connect+: reconocido como un dispositivo de creación de firmas cualificado
- Connect XC: compatible con BSI AIS 20/31

Conformidad con los estándares de seguridad y medioambientales

- UL, CE, FCC, RCM, ICES RoHS2 canadiense, WEEE

Alta disponibilidad

- Almacenamiento sólido
- Bandeja de campo, fuentes de administración intercambiables dobles

Administración supervisión

- Configuración remota nShield (disponible en modelos Connect XC configurados como consola de serie)
- nShield Remote Administration (comprado individualmente)
- nShield Monitor (comprado individualmente)
- Registro de auditoría seguro
- Soporte de diagnóstico Syslog y supervisión de rendimiento Windows
- Agente de supervisión SNMP

Características físicas

- Dimensiones de bastidor estándar 1U 19 pulgadas: 43,4 x 430 x 705 mm (1,7 x 16,9 x 27,8 pulgadas)
- Peso: 11,5 kg (25,4 libras)
- Voltaje de entrada: 100-240 V AC cambio automático 50-60 Hz
- Consumo de potencia: hasta 2.0 A a 110 V AC, 60 Hz | 1.0A a 220V AC, 50 Hz
- Disipación del calor: 327,6 a 362,0 BTU/hora (carga completa)
- Fiabilidad - MTBF (horas)[3], Connect XC: 107 384 horas, Connect+: 99 284 horas

Nota 3: calculada con una temperatura operativa de 25 °C utilizando el estándar MTBF "Procedimiento de predicción de fiabilidad para equipos electrónicos" de Telcordia SR-332.

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