

nShield Connect

- Maximiza el rendimiento y la disponibilidad con frecuencias de transacciones criptográficas altas y escalamiento flexible
- Compatible con una amplia variedad de aplicaciones incluyendo autorizaciones de certificados, firma de códigos y más
- nShield CodeSafe protege sus aplicaciones y lógica empresarial dentro del entorno de ejecución segura de nShield
- nShield Remote Administration y las opciones de Configuration y Monitor ayudan a reducir los viajes y administrar los HSM de manera más eficiente



HSM de nShield Connect

Aplicaciones certificadas que ofrecen servicios criptográficos claves, escalables y de alta disponibilidad a través de redes



HSM nShield Connect

Panorama de características



Los HSM nShield Connect son aplicaciones con certificación FIPS que proporcionan servicios criptográficos para aplicaciones en toda la red. Estas plataformas a prueba de manipulaciones indebidas realizan funciones de cifrado, firma digital y generación y protección de claves en una amplia gama de aplicaciones, incluidas las entidades de certificación, la firma de códigos, el software personalizado y más.

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

ARQUITECTURA ALTAMENTE FLEXIBLE

La exclusiva arquitectura Security World de nCipher le permite combinar modelos de HSM nShield y construir un estado mixto que ofrezca escalabilidad flexible, así como tolerancia a fallos y equilibrio de carga impecables.

PROCESE MÁS DATOS CON MAYOR RAPIDEZ

Los HSM nShield Connect son compatibles con frecuencias altas de transacción criptográfica, haciéndolos ideales para entornos empresariales, de distribución, el Internet de las cosas (IoT) y otros, donde la capacidad de procesamiento es crítica.

PROTEJA SUS DATOS Y APLICACIONES PATENTADAS

La opción de CodeSafe le proporciona un entorno seguro para ejecutar aplicaciones confidenciales dentro de los límites de nShield.

ESPECIFICACIONES TÉCNICAS

Algoritmos criptográficos compatibles

- Algoritmos asimétricos: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (incluidas las curvas NIST, Brainpool y 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 mensaje obtenido aplicando una función hash: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160
- Implementación de la Suite B con licenciamiento completo de curva elíptica ECC incluyendo Brainpool y curvas personalizadas

Sistemas operativos:

- Microsoft Windows 7 x64, 10 x64; Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- Red Hat Enterprise Linux AS / ES 6 x64, 6X86, 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
- Oracle Solaris 11 (SPARC), Oracle Solaris 11 x64
- IBM AIX 7.1 (POWER6, POWER8), HP-UX 11i v3
- Oracle Enterprise Linux 6.8 x64 y 7.1 x64

Interfaces de programación de aplicaciones (API)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI y CNG, nCore, nShield Web Services Crypto API

Conectividad de host

- Puertos Gigabit Ethernet duales (dos segmentos de red)

Cumplimiento con la seguridad

- Certificación FIPS 140-2 Nivel 2 y Nivel 3
- Certificación IPv6 y compatible con USGv6 Ready

Buscar: nCipherSecurity



©nCipher - febrero 2019 • PLB 8175

- Certificación Connect+: Common Criteria EAL4+ (AVA_VAN.5)
- Reconocimiento a Connect + como dispositivo de creación de firmas calificado
- Cumple con Connect XC: BSI AIS 20/31

Cumplimiento de normas de seguridad y medioambientales

- UL, CE, FCC, C-TICK, e ICES RoHS2, WEEE de Canadá

Disponibilidad alta

- Almacenamiento de estado sólido
- Componentes que se pueden reparar en el campo, fuentes de alimentación dobles de intercambio en caliente

Administración y Monitoreo

- nShield Remote Configuration (disponible en los modelos Connect XC configurados para la consola en serie)
- nShield Remote Administration (se compra por separado)
- nShield Monitor (se compra por separado)
- Registro de auditoría seguro
- Soporte de diagnóstico syslog y monitoreo de rendimiento de Windows
- Agente de monitoreo SNMP

Características físicas

- Estándar 1U 19 pulg. Dimensiones de montaje en bastidor: 43.4 x 430 x 705 mm (1.7 x 16.9 x 27.8 pulg)
- Peso: 11.5kg (25.4lb)
- Voltaje de entrada: 100-240V CA conmutación automática 50-60Hz
- Consumo de energía: hasta 2.0A a 110V CA, 60Hz | 1.0A a 220V AC, 50Hz
- Disipación de calor: 327.6 a 362.0 BTU/h (carga completa)

MODELOS DISPONIBLES Y RENDIMIENTO

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 bit	150	430	450	3,000	3,500	8,600
4096 bit	80 %	100	190	500	850	2,025
Rendimiento de firma de curva principal de ECC (tps) para longitudes de clave recomendadas por el NIST						
256 bit	540	680	1,260	2,400	5,500	14,400
Licencias para clientes						
Incluidas	3	3	3	3	3	3
Máximo	10	10	20	100	20	100

CONOZCA MÁS

Para obtener más información sobre cómo nCipher Security puede brindar confianza, integridad y control a la información y aplicaciones críticas de su negocio, visite ncipher.com