nCIPHER

CRYPTO STORE by ID-3

nShield Edge

- Maximiza la rentabilidad. nShield Edge es el HSM más económico en la familia nShield
- Compatible con una amplia variedad de aplicaciones y certificados de entidades, la firma de códigos y más
- Ofrece una fuerte seguridad. Los HSM de nShield Edge están certificados hasta FIPS 140-2 Nivel 3

HSM de nShield Edge

Dispositivos certificados conectados por USB que ofrecen servicios de claves criptográficas para aplicaciones de escritorio

HSM de nShield Edge

Características Generales

Los módulos de seguridad de hardware (HSM) de nShield Edge son dispositivos USB con todas las funciones, certificados por FIPS, que ofrecen cifrado, generación y protección de claves, además de conveniencia y economía.

DISEÑADO PARA ENTORNOS DE TRANSACCIONES DE BAJO VOLUMEN

Se adapta a entornos de generación y desarrollo de claves fuera de línea, al mismo tiempo que es compatible con un sinnúmero de algoritmos y API.

ALTAMENTE PORTÁTIL

Su diseño pequeño y ligero con interfaz USB es compatible con una variedad de plataformas, incluyendo computadoras portátiles y otros dispositivos móviles.

ECONÓMICO Y ESCALABLE

El HSM más económico de la familia nShield, nShield Edge le brinda un HSM de punto de entrada, con la opción de escalar su entorno a medida que aumentan sus necesidades. La arquitectura única de Security World de nCipher le permite combinar los modelos nShield HSM para crear un estado mixto que ofrece escalabilidad flexible, uso compartido de claves, perfecta tolerancia a fallos y equilibrio de carga.

ESPECIFICACIONES TÉCNICAS

Algoritmos Criptográficos Compatibles

- Algoritmos asimétricos: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, 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 Compatibles:

- Microsoft Windows 7 x64, 10 x64; Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- Red Hat Enterprise Linux AS/ES 6 x64, x86 y 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
- 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

Compatibilidad y capacidad de actualización

- Puerto USB (1.x, 2.x compatible)

Cumplimiento con la Seguridad

- FIPS 140-2 Nivel 2 y Nivel 3, y NIST SP 800-131A

Cumplimiento de las Normas de seguridad y Medio Ambiente

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

Administración y Seguimiento

- Control con operador remoto desatendido/de acceso multiusuario
- Registro de auditoría seguro
- Apoyo de diagnóstico syslog
- Monitoreo del rendimiento de Windows
- Agente de monitoreo SNMP

Características Físicas

- Dispositivo de escritorio portátil con lector de tarjeta inteligente integrado
- Dimensiones con soporte abierto 120 x 118 x 27 mm (4.7 x 4.6 x 1 pulg.)
- Peso: 340g (0.8lb)
- Voltaje de entrada: 5v CD alimentado por un dispositivo host USB
- Consumo de energía: 700mW

Rendimiento

- Rendimiento de firma para longitudes de clave recomendadas por NIST
- 2048 bit RSA: 2 tps
- 4096 bit RSA: 0.2 tps

MODELOS DISPONIBLES

- nShield Edge está disponible en FIPS Nivel 2 y Nivel 3
- También ofrece una edición sin FIPS para desarrolladores.

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 www.ncipher.com

Europe, UK - Oxford 7200, The Quorum, Oxford Business Park North, Garsington Road, Oxford, OX4 2JZ, United Kingdom • Tel: +44 (0) 1865 594724 • E-mail: enquires@id-3.co.uk