



ENTRUST

HSM nShield Edge

Dispositivos certificados con conexión USB que ofrecen servicios de claves criptográficas para aplicaciones de escritorio

PRINCIPALES CARACTERÍSTICAS

Los módulos de seguridad de hardware (HSM) de nShield Edge son dispositivos con todas las prestaciones, certificación FIPS y conexión USB que ofrece encriptación, generación y protección de claves de forma cómoda y económica.

- Maximiza la rentabilidad. nShield Edge es el HSM más económico de la familia nShield
- Compatible con una amplia variedad de aplicaciones incluyendo autoridades de certificado, firma de códigos y más
- Ofrece una fuerte seguridad. Los HSM nShield Edge tienen la certificación FIPS 140-2 de nivel 3

Diseñado para entornos de transacción de bajo volumen

Compatible con la generación de claves fuera de línea y los entornos de desarrollo, a la vez que ofrece soporte completo a los algoritmos y las API. Ideal para las implementaciones Bring Your Own Key (BYOK) que requieren la generación de claves criptográficas con garantía FIPS 140 de nivel 2 para exportarlas de forma segura a la nube.

Altamente portátil

Su diseño pequeño y ligero con una cómoda interfaz USB soporta una variedad de plataformas, incluyendo ordenadores portátiles y otros dispositivos portátiles.

Económico y escalable

El HSM más económico de la familia nShield, el nShield Edge le ofrece un HSM básico que le permite la opción de escalar su entorno a medida que aumenten sus necesidades. La arquitectura única de Security World de Entrust le permite combinar los modelos HSM nShield para crear un estado combinado que ofrece escalabilidad flexible, un sistema compartido de claves, migración en caso de falla y equilibrado de carga impecables.



APRENDA MÁS EN [ENTRUST.COM/HSM](https://www.entrust.com/hsm)

HSM nShield Edge

ESPECIFICACIONES TÉCNICAS

Algoritmos criptográficos soportados (incluida la implementación completa de NIST Suite B)	Sistemas operativos	Interfaces de programación de aplicaciones (API)	Compatibilidad y capacidad de actualización	Conformidad en seguridad
<ul style="list-style-type: none"> 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, 3DES Resumen de mensaje obtenido aplicando una función hash: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160 	<ul style="list-style-type: none"> Microsoft Windows 7 x64, 10 x64, Windows Server, 2012 R2 x64, 2016 x64, 2019 x64 Red Hat Enterprise Linux AS/ES 6 x64, x86 y 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64 Oracle Enterprise Linux 6.10 x64, 7.6 x64 	<ul style="list-style-type: none"> PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI y CNG, nCore, servicios web (requiere Web Services Option Pack) 	<ul style="list-style-type: none"> Puerto USB (compatible con 1.x, 2.x) 	<ul style="list-style-type: none"> FIPS 140-2 de nivel 2 y 3

Conformidad con los estándares de seguridad y medioambientales	Gestión y supervisión	Características físicas	Rendimiento
<ul style="list-style-type: none"> UL, CE, FCC, RCM, e ICES RoHS2 canadiense, WEEE 	<ul style="list-style-type: none"> Registro de auditoría seguro 	<ul style="list-style-type: none"> Dispositivo de sobremesa portátil con lector de tarjeta integrado Dimensiones con apertura 120 x 118 x 27 mm (4,7 x 4,6 x 1 pulgadas) Peso: 340 g (0,8 libras) Voltaje de entrada: 5v DC alimentados por un dispositivo USB Consumo de potencia: 700 mW 	<ul style="list-style-type: none"> Rendimiento de firma para las longitudes de clave recomendadas NIST: RSA 2048 bits: 2 tps RSA 4096 bits: 0,2 tps

MODELOS Y RENDIMIENTO DISPONIBLES

- El nShield Edge está disponible en variantes de FIPS de nivel 2 y nivel 3.
- También está disponible una edición para desarrollador no FIPS.

Más información

Para saber más sobre los HSM nShield de Entrust visite entrust.com/HSM. Para saber más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite entrust.com

Más información
entrust.com/HSM



Contacte con nosotros:
HSMinfo@entrust.com