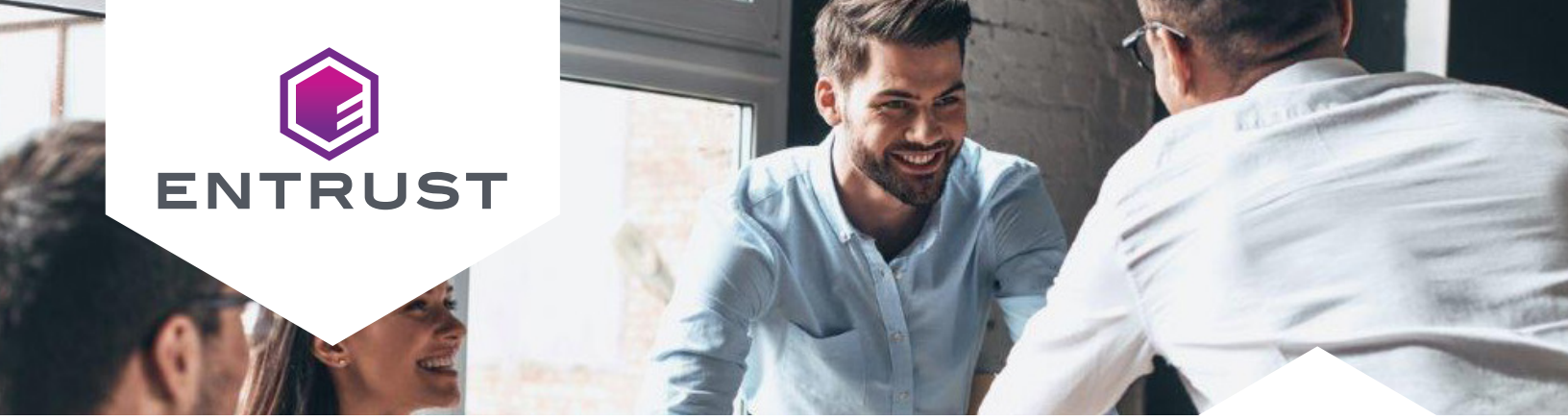


HSM nShield Solo

Tarjetas PCI Express certificadas que ofrecen servicios de claves criptográfica para servidores individuales

CARACTERÍSTICAS PRINCIPALES

Los módulos de seguridad de hardware (HSM) nShield Solo son tarjetas PCI-Express con certificación FIPS de perfil bajo que ofrecen servicios criptográficos a aplicaciones alojadas en un servidor o dispositivo. Estas tarjetas resistentes a falsificaciones realizan funciones como encriptación, firma digital y generación y protección de claves para un amplio abanico de aplicaciones, incluyendo autoridades de certificación, firma de código, software personalizado y mucho más.

La serie nShield Solo incluye nShield Solo+ y el nuevo nShield Solo XC de alto rendimiento.

Arquitectura altamente flexible

La arquitectura única de Security World nCipher 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

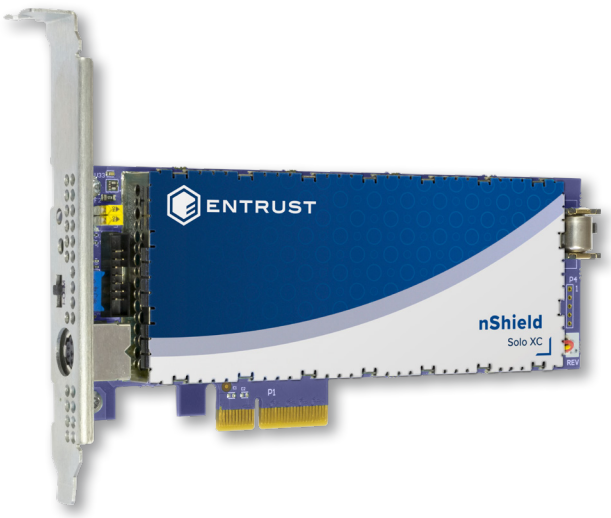
Los HSM nShield Solo soportan altas tasas de transacción, lo que los hace perfectos para empresas, comercio minorista, Internet de las cosas y otros entornos donde la capacidad de procesamiento es fundamental.

Proteja sus aplicaciones y datos privados

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

ASPECTOS CLAVE Y BENEFICIOS

- Maximiza el rendimiento y la disponibilidad apoyando un alto número de transacciones criptográficas y escalamiento flexible
- Soporta una amplia variedad de aplicaciones incluyendo autoridades de certificado, firma de códigos y más
- CodeSafe nShield protege sus aplicaciones dentro del entorno de ejecución segura nShield
- La administración remota de nShield le ayuda a reducir los gastos y reducir los viajes



APRENDA MÁS EN ENTRUST.COM/HSM

HSM nShield Solo

ESPECIFICACIONES TÉCNICAS

Algoritmos criptográficos soportados

- 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 mensajes/algoritmos hash: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160
- Implementación total de Suite-B con criptografía de curva elíptica (ECC) completamente autorizada incluyendo Brainpool y curvas personalizadas

Plataformas soportadas

- Sistemas operativos Windows y Linux, incluidas las distribuciones de RedHat, SUSE y los principales proveedores de servicios en la nube que se ejecutan como máquinas virtuales o en contenedores
- Los entornos virtuales de Solo XC soportados incluyen VMware ESX, Microsoft Hyper-V, Linux KVM y Citrix XenServer

Interfaces de programación de aplicaciones (API)

- PKCS # 11, OpenSSL, Java (JCE), Microsoft CAPI y CNG, nCore, y Web Services (requiere Web Services Option Pack)

Conectividad de servidor

- Versión PCI Express 2.0; conector Solo+: 1 vía, conector Solo XC: 4 vías

Conformidad en seguridad

- Certificación FIPS 140-2 de nivel 2 y 3
- Solo+: certificación Common Criteria EAL4+ (AVA_VAN.5)
- Solo+ reconocido como un dispositivo de creación de firmas cualificado
- Solo 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
- Solo XC: cumple con BSI AIS 20/31

Conformidad con los estándares de seguridad y medioambientales

- UL, UL/CA, CE, FCC, y de Canadá ICES, KC, FCC, VCCI, RCM
- RoHS2, WEEE, REACH

Gestión y supervisión

- nShield Remote Administration y nShield Monitor
- Registro de auditoría seguro
- Soporte de diagnóstico Syslog y supervisión de rendimiento Windows
- Agente de supervisión SNMP

MODELOS DISPONIBLES Y RENDIMIENTO

Modelos nShield Solo	500+	XC Base	6000+	XC Medio	XC Alto
Rendimiento de firma RSA (tps) para longitudes de clave recomendadas por NIST					
2048 bits	150	430	3000	3500	8600
4096 bits	80	100	500	850	2025
Rendimiento de firma de ECC principal (tps) para las longitudes de clave recomendadas NIST					
256 bits	540	680	2400	7515[1]	14 400[1]

Dimensiones	Peso		Energía	
	Solo+	Solo XC	Solo+	Solo XC
56,2 Q 167,1 Q 15,4mm	230 g	280 g	10 W	24 W
2,2 Q 6,6 Q 0,6 pulgadas	0,5 libras	0,62 libras		

Nota 1: el rendimiento indicado requiere la activación de la función rápida RNG de ECDSA disponible de forma gratuita a petición del soporte de nCipher.

Más información
entrust.com/HSM

ENTRUST

Contacte con nosotros:
HSMinfo@entrust.com