NCIPHER

www.ncipher.com

nShield Solo

- Maximiza el rendimiento y la disponibilidad apoyando un alto número de transacciones criptográficas y escalamiento flexible
- Compatible con una amplia variedad de aplicaciones incluyendo autorizaciones de certificados, firma de código y más
- Protege sus aplicaciones más sensibles dentro del entorno de ejecución segura de nShield CodeSafe
- nShield Remote Adminstration le ayuda a reducir costos y viajes

HSM nShield Solo

Tarjetas PCI-Express certificadas que proporcionan servicios de claves criptográficas a servidores independientes

HSM nShield Solo

Características Generales

Los módulos de seguridad de hardware (HSM) nShield Solo son tarjetas PCI-Express certificadas por FIPS de bajo perfil que ofrecen servicios criptográficos para aplicaciones alojadas en servidores y dispositivos. Estas tarjetas 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 nShield Solo incluye nShield Solo+ y el nuevo diseño de más alto rendimiento nShield Solo XC.

ARQUITECTURA ALTAMENTE FLEXIBLE

La exclusiva arquitectura Security World de nCipher le permite combinar los diferentes modelos de HSM nShield para construir un estado mixto que ofrezca escalabilidad flexible y balanceo de cargas sin fisuras.

PROCESE MÁS DATOS CON MAYOR RAPIDEZ

Los HSM nShield Solo apoyan un alto nivel de transacciones, siendo una solución ideal para aplicaciones corporativas, de distribución, de IoT y otros entornos donde el rendimiento es crítico.

PROTEJA SUS DATOS Y APLICACIONES PATENTADAS

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

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:

- Microsoft Windows 7 x64, 10 x64; Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- Red Hat Enterprise Linux AS/ES 6 x64, 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
- Oracle Solaris 11 (SPARC), Oracle Solaris 11 x64
- Solo+: Red Hat Enterprise Linux AS/ES 6 x86, IBM AIX 7.1 (POWER6), HP-UX 11i v3`
- Oracle Enterprise Linux 6.8 x64 y 7.1 x64
- Compatibilidad con el entorno virtual Solo XC: Microsoft Windows Hyper-V Server 2016, VMware ESXi 6.5, Citrix XenServer 6.5

Interfaces de programación de aplicaciones (API)

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

Conectividad del host

- PCI Express versión 2.0; Solo+ conector: 1 carril, Solo XC conector: 4 carriles

Cumplimiento con la seguridad

- Certificación FIPS 140-2 Nivel 2 y Nivel 3
- Solo+: certificado Common Criteria EAL4 + (AVA_VAN.5)
- Reconocimiento a Solo+ como un dispositivo de creación de firmas calificado
- Solo XC: cumple con BSI AIS 20/31

Cumplimiento de las Normas de Seguridad y Medio Ambiente

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

Administración y Monitoreo

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

Dimensiones	Peso		Energía	
	Solo+	Solo XC	Solo+	Solo XC
56.2 × 167.1 × 15.4mm	230g	280g	10W	24W
2.2 × 6.6 × 0.6pulg.	0.5lb	0.62lb		

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 bit	150	430	3,000	3,500	8,600
4096 bit	80 %	100 %	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	2,400	5,500	14,400

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

Buscar: nCipherSecurity