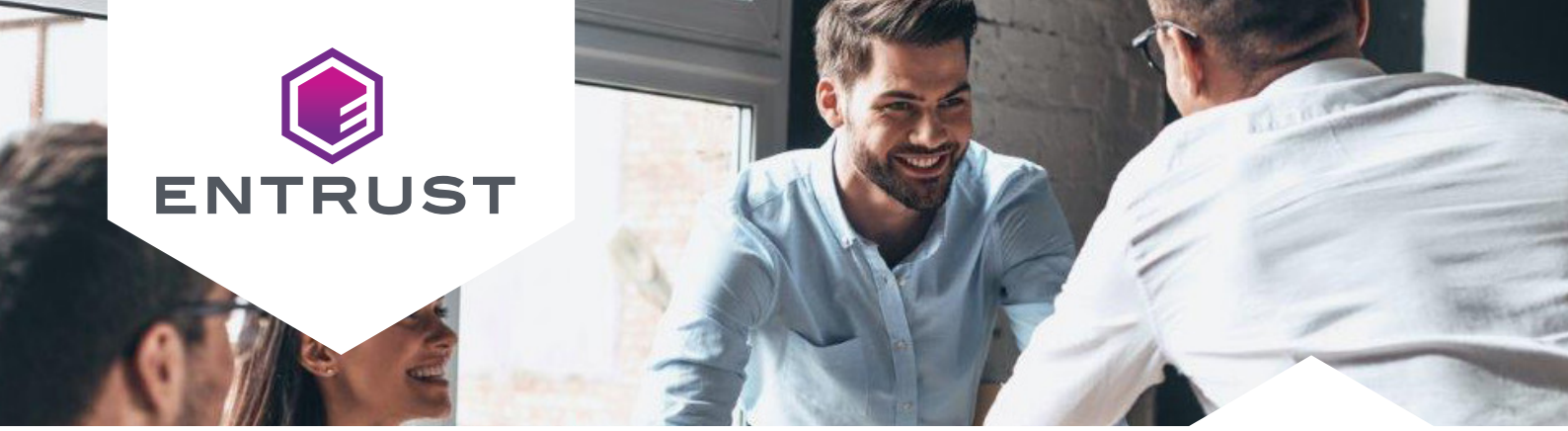


nShield Solo HSM

Zertifizierte PCI-Express-Karten, die kryptographische Schlüsseldienste für eigenständige Server bereitstellen

HIGHLIGHTS

nShield Solo Hardware-Sicherheitsmodule (HSM) sind FIPS-zertifizierte PCI-Express-Karten, die kryptographische Schlüsseldienste für Anwendungen bereitstellen, die auf Servern oder Geräten gehostet werden. Diese manipulationssicheren Karten bieten Funktionen wie Verschlüsselung, digitale Signierung sowie Schlüsselerstellung und -schutz für eine Vielzahl an Anwendungen, einschließlich Zertifizierungsstellen, Code Signing, benutzerdefinierte Software und mehr.

Die nShield Solo-Reihe umfasst nShield Solo+ und das neue, leistungsstarke nShield Solo XC.

Hochflexible Architektur

Mit der einzigartigen Security-World-Architektur von nCipher können Sie die nShield-HSM-Modelle zum Aufbau einer gemischten Infrastruktur kombinieren, die flexible Skalierbarkeit sowie nahtlosen Failover und Lastenausgleich bietet.

Mehr Daten schneller verarbeiten

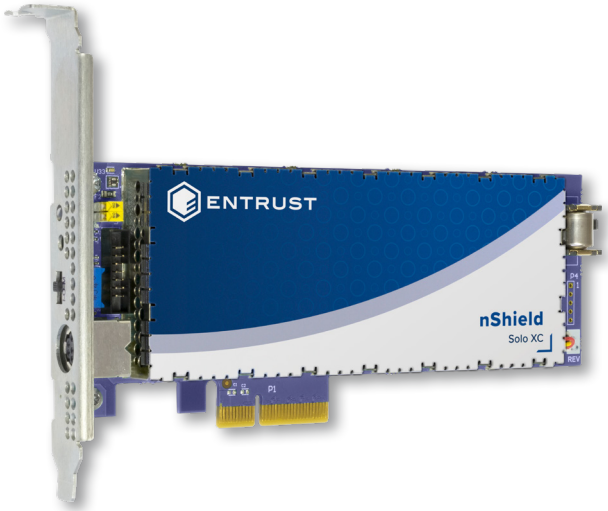
nShield Solo HSMs unterstützen hohe Transaktionsraten und sind daher ideal für Unternehmen, Einzelhandel, IoT- und andere Umgebungen geeignet, in denen der Durchsatz entscheidend ist.

Schützen Sie Ihre proprietären Anwendungen und Daten

Die Option CodeSafe bietet eine sichere Umgebung für die Ausführung sensibler Anwendungen innerhalb von nShield.

WICHTIGE FUNKTIONEN UND VORTEILE

- Maximiert Performance und Verfügbarkeit durch hohe kryptographische Transaktionsraten und flexible Skalierbarkeit
- Unterstützt eine Vielzahl an Anwendungen wie Certificate Authorities, Code Signing und mehr
- nShield CodeSafe schützt Ihre Anwendungen innerhalb der sicheren Ausführungsumgebung von nShield
- nShield Remote Administration reduziert Kosten und Reiseaufwand



WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

nShield Solo HSM

TECHNISCHE DATEN

Unterstützte kryptographische Algorithmen

- Asymmetrische Algorithmen: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- Symmetrische Algorithmen: 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
- Hash-/Hashwert: MD5, SHA-1, SHA-2 (224, 256, 384, 512 Bit), HAS-160, RIPEMD 160
- Vollständige Suite-B-Implementierung mit voll lizenziertem ECC, inklusive Brainpool und benutzerdefinierten Kurven

Unterstützte Plattformen

- Windows- und Linux-Betriebssysteme einschließlich Distributionen von RedHat, SUSE und großen Cloud-Anbieter, die als virtuelle Maschinen oder Container ausgeführt werden
- Zu den von Solo XC unterstützten virtuellen Umgebungen gehören VMware ESX, Microsoft Hyper-V, Linux KVM und Citrix XenServer

Anwendungsprogrammier-Schnittstellen (APIs)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI und CNG, nCore und Web Services (erfordert das Web Services Option Pack)

Host-Konnektivität

- PCI Express Version 2.0; Solo+-Connector: 1 lane, Solo-XC-Connector: 4 lane

Sicherheits-Compliance:

- Nach FIPS 140-2 Level 2 und Level 3 zertifiziert
- Nach Common Criteria EAL4+ (AVA_VAN.5) zertifiziert
- Solo+ ist als qualifiziertes Signaturerstellungsgerät (Qualified Signature Creation Device) anerkannt
- Solo XC: eIDAS und Common Criteria EAL4 + AVA_ VAN.5 und ALC_ FLR.2-Zertifizierung gemäß dem Schutzprofil EN 419 221-5 laut dem niederländischen NSCIB-System
- Solo XC: BSI-AIS-20/31-konform

Einhaltung von Sicherheits- und Umweltstandards

- UL, UL/CA, CE, FCC, ICES (Kanada), KC, FCC, VCCI, RCM
- RoHS2, WEEE, REACH

Verwaltung und Überwachung

- nShield-Remote Administration und nShield-Monitor
- Sichere Audit-Protokollierung
- Syslog-Diagnose-Unterstützung und Windows Leistungsüberwachung
- Agent für SNMP-Überwachung

VERFÜGBARE MODELLE UND LEISTUNG

nShield Solo-Modelle	500+	XC Base	6000+	XC Mid	XC High
RSA Signing Performance (tps) für NIST Empfohlene Schlüssellängen					
2048 Bit	150	430	3.000	3.500	8.600
4096 Bit	80	100	500	850	2.025
ECC Prime Curve Signing Performance (tps) für NIST Empfohlene Schlüssellängen					
256 Bit	540	680	2.400	7.515[1]	14.400[1]

Maße	Gewicht		Leistung	
	Solo+	Solo XC	Solo+	Solo XC
56,2 × 167,1 × 15,4mm	230g	280g	10W	24W
2,2 × 6,6 × 0,6in	0,5lb	0,62lb		

Hinweis 1: Die angegebene Performance erfordert die schnelle Aktivierung der RNG-Funktion von ECDSA, die der Support von nCipher kostenlos zur Verfügung stellt.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com