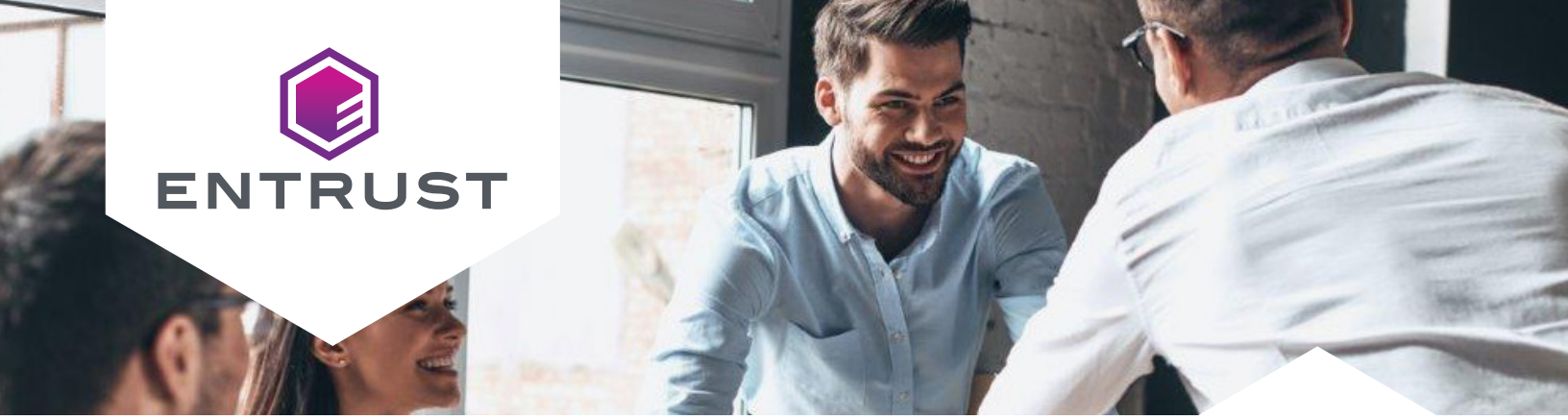


nShield Solo HSMs

Certified PCI-Express cards that deliver cryptographic key services to stand-alone servers

HIGHLIGHTS

nShield Solo hardware security modules (HSMs) are FIPS-certified, low-profile PCI-Express cards that deliver cryptographic services to applications hosted on a server or appliance. These tamper-resistant cards perform such functions as encryption, digital signing and key generation and protection over an extensive range of applications, including certificate authorities, code signing, custom software and more.

The nShield Solo series includes nShield Solo+ and the new, high-performance nShield Solo XC.

Highly flexible architecture

nCipher unique Security World architecture lets you combine nShield HSM models to build a mixed estate that delivers flexible scalability and seamless failover and load balancing.

Process more data faster

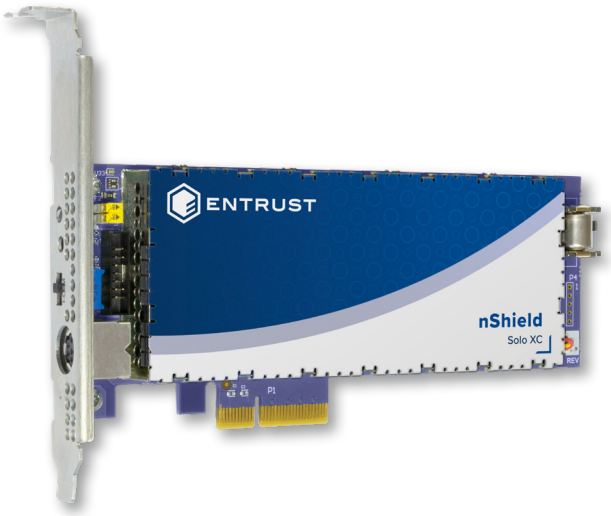
nShield Solo HSMs support high transaction rates, making them ideal for enterprise, retail, IoT and other environments where throughput is critical.

Protect your proprietary applications and data

The CodeSafe option provides a secure environment for running sensitive applications within nShield boundaries.

KEY FEATURES & BENEFITS

- Maximize performance and availability with high cryptographic transaction rates and flexible scaling
- Supports a wide variety of applications including certificate authorities, code signing and more
- nShield CodeSafe protects your applications within nShield's secure execution environment
- nShield Remote Administration helps you cut costs and reduce travel



LEARN MORE AT ENTRUST.COM/HSM

nShield Solo HSMs

TECHNICAL SPECIFICATIONS

Supported cryptographic algorithms

- Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- Symmetric algorithms: 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/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160
- Full Suite B implementation with fully licensed ECC, including Brainpool and custom curves

Supported platforms

- Windows and Linux operating systems including distributions from RedHat, SUSE and major cloud service providers running as virtual machines or in containers
- Solo XC virtual environments supported including VMware ESX, Microsoft Hyper-V, Linux KVM & Citrix XenServer

Application programming interfaces (APIs)

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

Host connectivity

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

Security compliance

- FIPS 140-2 Level 2 and Level 3 certified
- Solo+: Common Criteria EAL4+ (AVA_VAN.5) certified
- Solo+ recognized as a Qualified Signature Creation Device
- Solo XC: eIDAS and Common Criteria EAL4 + AVA_VAN.5 and ALC_ FLR.2 certification against EN 419 221-5 Protection Profile, under the Dutch NSCIB scheme
- Solo XC: BSI AIS 20/31 compliant

Safety and environmental standards compliance

- UL, UL/CA, CE, FCC, Canada ICES, KC, FCC, VCCI, RCM
- RoHS2, WEEE, REACH

Management and monitoring

- nShield Remote Administration and nShield Monitor
- Secure audit logging
- Syslog diagnostics support and Windows performance monitoring
- SNMP monitoring agent

AVAILABLE MODELS AND PERFORMANCE

nShield Solo models	500+	XC Base	6000+	XC Mid	XC High
RSA signing performance (tps) for NIST recommended key lengths					
2048 bit	150	430	3,000	3,500	8,600
4096 bit	80	100	500	850	2,025
ECC prime curve signing performance (tps) for NIST recommended key lengths					
256 bit	540	680	2,400	7,515[1]	14,400[1]

Dimensions	Weight		Power	
	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		

Note 1: Performance indicated requires ECDSA fast RNG feature activation available free of charge on request from nCipher support.

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com