DATA SHEET

Entrust nShield® Solo HSMs

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

HIGHLIGHTS

Entrust 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 support key generation and strong protection when not in use, while providing a secure environment for cryptographic functions such as encryption and digital signing for an extensive range of applications, including certificate authorities, code signing, custom software, and more.

Post-Quantum Support

nShield Solo HSMs support NIST-standardized quantum-resistant algorithms, paving the way for resilient security in the post-quantum era.

Highly Flexible Architecture

The nShield 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

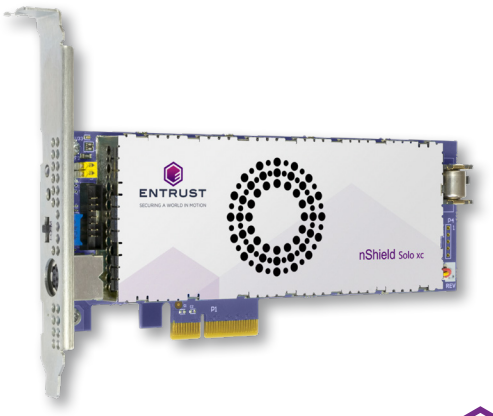
The CodeSafe option provides a secure environment for running sensitive applications within nShield boundaries.

Seamless Integration

The Entrust **Cryptographic Security Platform** provides a root of trust for key and secrets management, PKI, and certificate lifecycle management

Central Management, Configuration, and Monitoring

The nShield KeySafe 5 utility provides the central management, configuration, and monitoring of an estate of HSMs and related Security Domains through an intuitive web-based UI and RESTful APIs.



ENTRUST
SECURING A WORLD IN MOTION

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 option helps you cut costs and reduce travel

Technical Specifications

Supported cryptographic algorithms	Supported platforms	Application programming interfaces (APIs)
• NIST standardized post-quantum algorithms: ML-DSA-44, ML-DSA-65, ML-DSA-87, ML-KEM-512, ML-KEM-768, ML-KEM-1024, SLH-DSA-SHA2-128f, SLH-DSA-SHA2-128s, SLH-DSA-SHAKE-128f, SLH-DSA-SHAKE-128s, SLH-DSA-SHA2-192f, SLH-DSA-SHA2-192s, SLH-DSA-SHAKE-192f, SLH-DSA-SHAKE-192s, SLH-DSA-SHA2-256f, SLH-DSA-SHA2-256s, SLH-DSA-SHAKE-256f, SLH-DSA-SHAKE-256s • Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph) • Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, 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 • Elliptic Curve Key Agreement (ECKA) available via Java API and nCore APIs Elliptic Curve Integrated Encryption Scheme (ECIES) available via Java API, PKCS#11, and nCore APIs • LMS and additional PQC algorithm support (requires Post-Quantum Option Pack)	• Windows and Linux operating systems including distributions from Red Hat, 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	• PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore, and Web Services (requires nShield Web Services Option Pack)

Host connectivity	Security compliance	Safety, EMC, & environmental compliance	Management and monitoring
• PCI Express Version 2.0; Solo XC connector: 4 lane	• FIPS 140-2 Level 2 and Level 3 certified • Recognized as a Qualified Signature Creation Device • 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 • BSI AIS 20/31 compliant	• UL/CA, CE, FCC, Canada ICES, KC, VCCI, RCM, UKCA • RoHS, WEEE, REACH	• nShield Remote Administration • KeySafe 5 utility for central management, configuration, and monitoring of HSM estate • Secure audit logging • Syslog diagnostics support and Windows performance monitoring • SNMP monitoring agent

Available Models and Performance

nShield Connect Models	XC Base	XC Mid	XC High
RSA signing performance (tps) for NIST recommended key lengths			
2048 bit	430	3,500	8,600
4096 bit	100	850	2,025
8192 bit	19	115	309
ECC prime curve signing performance (tps) for NIST recommended key lengths			
256 bit	680	7,515[2]	14,400[2]
Symmetric encryption (KB/sec) 1024 byte plain text			
3 DES 168 bit	685	5,140	5,500
AES 128 bit	825	7,700	11,300
Key generation (keys/sec)			
RSA 2048 bit	6.0	6.2	7.3
ECDSA P-192 bit[1]	110	650	1,050
ECDSA P-256 bit[1]	100	630	1,050
ECDSA P-521 bit[1]	65	480	710

Each nShield Solo XC is supplied with an external smart card reader. Compatible smart cards are available to order separately.

1: Requires ECC activation

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION