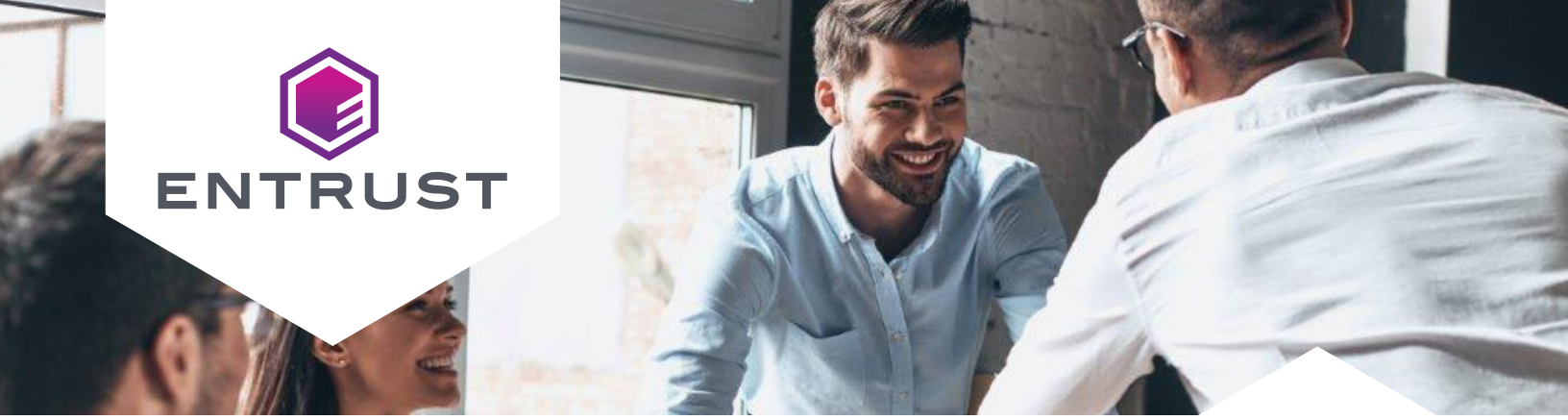


Entrust nShield® Solo HSMs

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.

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.

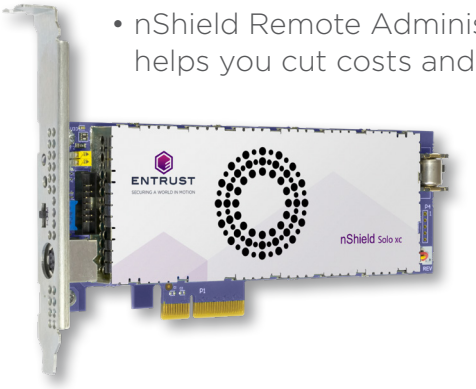
Furthermore, with CodeSafe the optional Post Quantum SDK supports NIST's PQC algorithms identified for standardization.

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;

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



Learn more about nShield HSMs at Entrust.com

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, 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
- NIST's PQC algorithms identified for standardization including CRYSTALS-Dilithium, FALCON, and SPHINCS+ digital signature algorithms (requires CodeSafe PQ SDK)

Supported platforms

- 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

Application programming interfaces (APIs)

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

Host connectivity

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

Security compliance

- 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

Safety, EMC, & environmental compliance

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

Management and monitoring

- nShield Remote Administration and nShield Monitor
- 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
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.
Note 1: Requires ECC activation

Learn more about nShield HSMs at Entrust.com

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted experiences for identities, payments, and digital infrastructure. We offer an unmatched breadth of solutions that are critical to enabling trust for multi-cloud deployments, mobile identities, hybrid work, machine identity, electronic signatures, encryption, and more. With more than 2,800 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact