Entrust nShield® 5s HSMs

High-performance, next-generation, crypto-agile PCIe hardware security modules

HIGHLIGHTS

Comprehensive capabilities

Entrust nShield® 5s hardware security modules (HSMs) are FIPS 140-3 Level 3 certified and Common Criteria EAL4+ (EN 419 221-5) certified low-profile PCIe cards that deliver cryptographic services to applications hosted on a server or appliance.

- Maximize performance and availability with high cryptographic transaction rates and flexible scaling
- Supports a wide variety of applications including certificate authorities, code signing, 5G, and more
- FIPS 140-3 certified
- nShield Remote Administration option helps you cut costs and reduce travel
- Designed for multi-tenancy support

nShield 5s HSMs are tamper-resistant devices that perform functions such as encryption, digital signing, and key generation supporting a range of applications and technologies, such as:

- Certificate authorities
- Code signing
- Custom software
- Cloud and containerized applications
- Web services
- Remote signing
- Blockchain
- Database encryption
- 5G for telco environments
- IoT applications
- Car2X

Learn more at entrust.com/HSM

nShield 5s HSMs

KEY FEATURES & BENEFITS

Highly flexible architecture

nShield 5s is the latest addition to the range of HSMs that fit seamlessly with Entrust's unique Security World architecture. Entrust Security World 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 5s HSMs support high transaction rates, making them ideal for application environments where throughput is critical. In field performance upgrades available through software license avoiding unnecessary hardware swap outs.

Centralized remote management

KeySafe 5, available with Security World software, allows organizations to centrally manage their estate of HSMs and associated Security Worlds remotely.

Maximize application security

The CodeSafe software developer toolkit provides the capability to create and execute sensitive applications within the protected perimeter of a FIPS 140-3 Level 3 certified nShield hardware security module (HSM).

POWERFUL NSHIELD 5 REMOTE OPTIONS

Eliminate visits to the data center

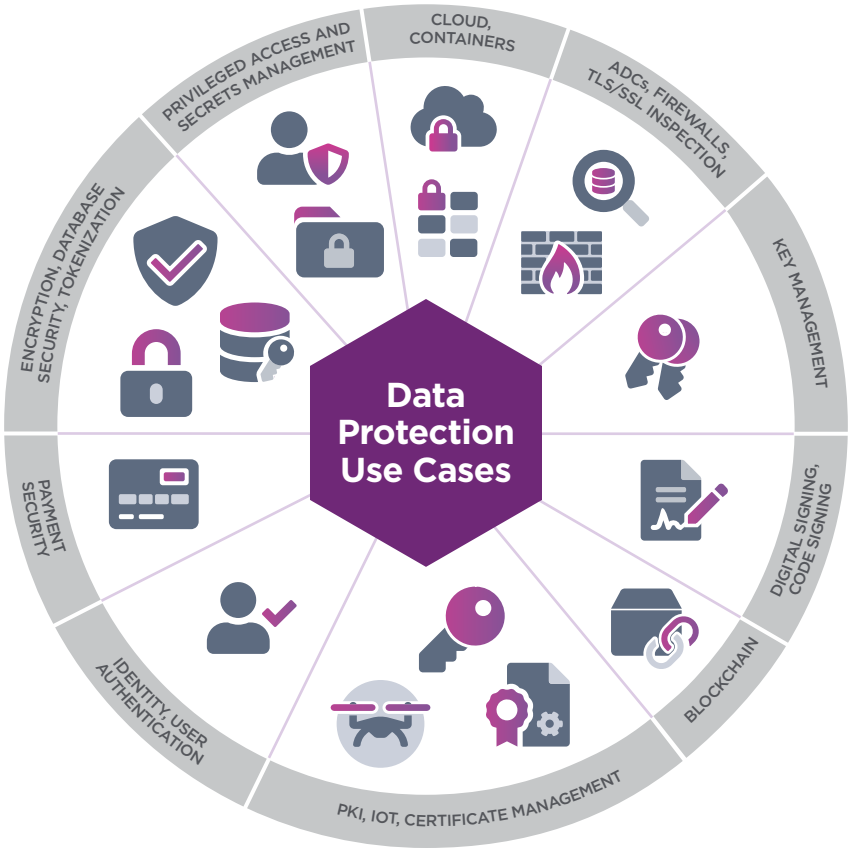
nShield Remote Administration – Enables the secure remote presentation of authorization smart cards to remote HSMs to execute maintenance tasks including enrolling new HSMs and reassigning/ reconfiguring existing HSMs. Separate data sheet available.

Remote Configuration – Serial console allows simple installation for data center staff, and allows HSM and client configuration without requiring physical access to the HSM front panel and front panel settings.

Crypto-agility – Field-programmable, secure cryptographic accelerator, which offers the flexibility to implement new security measures and algorithms (e.g. PQC algorithms) via firmware upgrade, safeguarding investment and reducing total cost of ownership.

nShield 5s HSMs

Entrust nShield HSMs provide high assurance security for a broad range of use cases



AVAILABLE MODELS AND PERFORMANCE

nShield 5s models	Base	Mid	High
RSA signing performance (tps) for NIST recommended key lengths			
2048 bit	670	3,949	13,614
4096 bit	135	814	2,200
8192 bit	19	115	309
ECC prime curve signing performance (tps) for NIST recommended key lengths			
256 bit	2,085	7,553	21,826
512 bit	1010	5,977	16,164
Key generation (keys/sec)			
RSA 2048 bit	7	20	23
ECDSA P-256 bit	1,040	3,580	3,494
ECDSA P-521 bit	518	2,480	2,724
Key agreement performance (transactions/sec)			
ECDSA P-256 bit	2,085	7,550	21,436

Each nShield 5s HSM is supplied with an external smart card reader for local use.

Learn more at entrust.com/HSM

nShield 5s HSMs

TECHNICAL SPECIFICATIONS

Supported cryptographic algorithms

- Full NIST Suite B implementation
- Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- Symmetric algorithms: AES, Arcfour, ARIA, Camellia, 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, SHA-3 (224, 256, 384, 512 bit)
- 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
- TUAK and MILENAGE algorithm support for mutual authentication and key generation (3GPP)
- NIST short-listed post-quantum cryptographic algorithms supported using the nShield Post-Quantum CodeSafe WITH Option Pack

Supported platforms

- Windows and Linux operating systems including distributions from Red Hat, SUSE

Application programming interfaces (APIs)

- PKCS#11
- OpenSSL
- Java (JCE)
- Microsoft CAPI/CNG
- Web Services
- nCore

Host connectivity

- PCIe Version 2.0; connector: 4 lane

Security compliance

- FIPS 140-3 Level 3
- BSI AIS 20/31 compliant
- eIDAS and Common Criteria EAL4+

Safety and environmental standards compliance

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

Management and monitoring

- KeySafe 5 and nShield Remote Administration
- Secure audit logging
- Syslog diagnostics support and Windows performance monitoring
- SNMP monitoring agent

Physical characteristics

- Dimensions: 167.7mm x 68.9mm (excludes mounting bracket dimensions)
- Weight: 270g
- Power: 25W
- Reliability – MTBF[1]: 1,702,841 hours
- Mounting bracket – supplied with low-profile (fitted) and full-height bracket

Note 1: Calculated at 25 degrees centigrade operating temperature using Telcordia SR-332 "Reliability Prediction Procedure for Electronic Equipment" MTBF Standard

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