

Entrust nShield® 5c HSMs

High-performance, PQ-secure, next-generation, and crypto-agile hardware security modules

HIGHLIGHTS

Comprehensive Capabilities

Entrust nShield® 5c Hardware Security Modules (HSMs) are FIPS 140-3 Level 3 certified and Common Criteria EAL4+ (EN 419 221-5) certified appliances that deliver scalable and highly available cryptographic key services across networks.

- Future-proof with post-quantum algorithm support and hardware acceleration
- Integrate with more than 150 leading application provider solutions
- Powerful remote configuration and management capability following simple installation
- Integration with Entrust **Cryptographic Security Platform** provides root of trust for key and secrets management, PKI, and certificate lifecycle management

nShield 5c 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 telecoms
- IoT applications
- Car2X



nShield 5c



nShield 5c 10G

KEY FEATURES & BENEFITS

Post-Quantum Support

nShield 5c HSMs support NIST's quantum-resistant algorithms, offering robust security in a post-quantum world. Future-proof against post-quantum threats with firmware upgradeable hardware acceleration for current and future algorithms.

Highly Flexible Architecture

nShield 5c 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 5 HSMs support high transaction rates, making them ideal for enterprise application environments where throughput is critical. nShield 5 HSMs also support in-field performance upgrades delivered via firmware upgrades, 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 World architecture 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 HSM.

Remote Features 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. [See data sheet.](#)

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 supports loading multiple FPGA images, enabling optimized hybrid and PQC cryptographic operations. This upgradeable design delivers flexibility to adopt new algorithms, safeguards long-term investment, and reduces total cost of ownership.

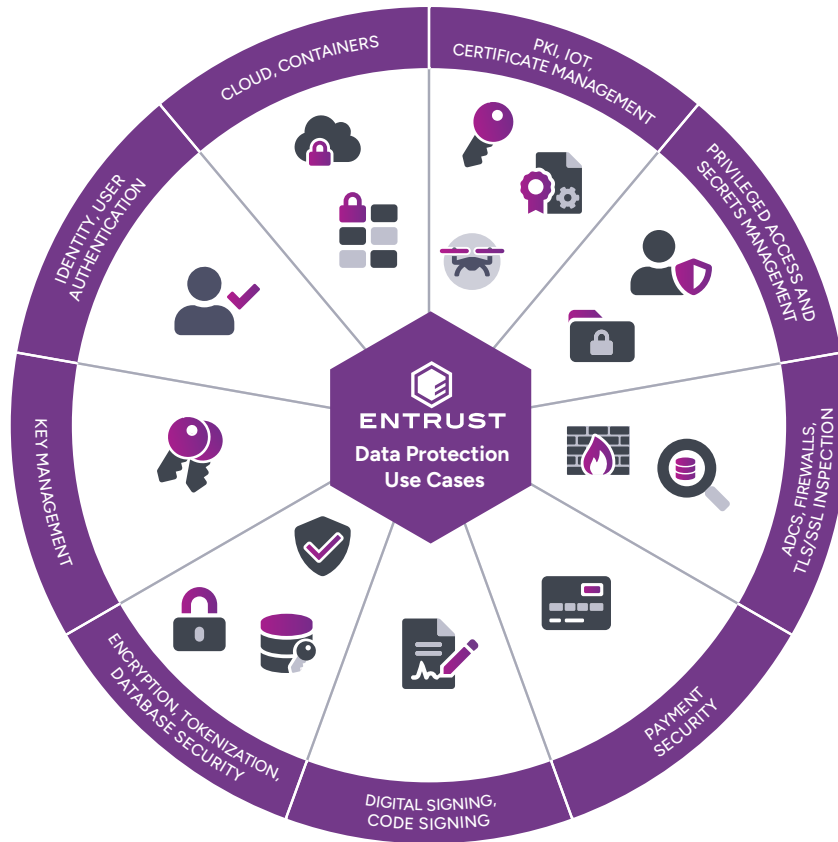
Key and Secrets Management

nShield 5c can be integrated with the Entrust Cryptographic Security Platform Key Management Solution. The HSM protects the master key for the key management platform and also generates high-quality cryptographic keys using a hardware-based random number generator.



nShield 5c 10G - detail of network interface

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



Available Models and Performance

Performance results are indicative, based on testing with firmware version 13.8.3 in Hybrid Hardware Accelerated Mode under lab conditions. Customer environment performance may vary.

nShield 5c Models	Base	Mid	High
ML-DSA signing performance (tps) for NIST standardized PQC schemes			
ML-DSA44	380	890	3,130
ML-DSA65	270	620	2,160
ML-DSA87	230	520	1,770
RSA signing performance (tps) for NIST recommended key lengths			
2048 bit	580	3,460	11,680
4096 bit	110	680	2,050
8192 bit	15	95	310
ECC prime curve signing performance (tps) for NIST recommended key lengths			
256 bit	2,070	7,530	23,890
512 bit	850	5,110	14,360

Available Models and Performance - Continued

nShield 5c Models	Base	Mid	High
Key generation (keys/sec)			
RSA 2048 bit	10	50	70
ECDSA P-256 bit	2,060	3,700	3,790
ECDSA P-521 bit	860	3,040	3,090
Key agreement performance (transactions/sec)			
ECDH P-256 bit	2,080	7,540	21,970
Client licenses¹			
Included	3	3	3
Maximum	10	20	1000

1: From Security World v13.6 onwards - Client licenses are counted as simultaneous active connections.

Technical Specifications

Supported cryptographic algorithms	Supported platforms	Application programming interfaces (APIs)	Host connectivity	Security compliance
<ul style="list-style-type: none"> 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 (including NIST, Brainpool & secp256k1 curves), ECDH, Edwards (Ed25519, Ed25519ph) Symmetric algorithms: AES, AES-GCM, 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) Additional NIST PQ algorithms, not detailed above, such as LMS supported using the nShield Post-Quantum Option Pack 	<ul style="list-style-type: none"> Windows and Linux operating systems including distributions from Red Hat, SUSE, and major cloud service providers running as virtual machines or in containers 	<ul style="list-style-type: none"> PKCS#11 OpenSSL Java (JCE) Microsoft CAPI/CNG Web Services nCore 	<p>nShield 5c</p> <ul style="list-style-type: none"> Dual Gigabit Ethernet ports (two network segments with network bonding option) <p>nShield 5c 10G</p> <ul style="list-style-type: none"> 10 Gigabit (four SFP+ ports with network bonding options) SFP+ Transceiver options: <ul style="list-style-type: none"> Fiber 850nm short range Fiber 1310nm long range Copper RJ-45 	<ul style="list-style-type: none"> FIPS 140-3 Level 3 eIDAS and Common Criteria EAL4+ True Random Number Generator (TRNG) certified to AIS 20/31 and NIST SP 800-90B

Technical Specifications

Safety, EMC & environmental compliance	High availability	Management and monitoring	Physical characteristics
<ul style="list-style-type: none"> • UL, CE, FCC, UKCA, RCM, Canada ICES • RoHS, WEEE, REACH 	<ul style="list-style-type: none"> • All solid-state storage • Field serviceable fan tray • Dual hot-swap power supplies • Full support for clustering HSMs and automated failover/load balancing • Network bonding supporting active backup mode and 802.3ad mode 	<ul style="list-style-type: none"> • KeySafe 5, nShield Remote Configuration • nShield Remote Administration (purchased separately) • Secure audit logging • Syslog diagnostics support and Windows performance monitoring • SNMP monitoring agent 	<ul style="list-style-type: none"> • Standard 1U 19in. rack mount • Dimensions: <ul style="list-style-type: none"> • nShield 5c: 43.4 x 430 x 705mm (1.7 x 16.9 x 27.8in) • nShield 5c 10G: 42.6 x 431 x 720 (1.7 x 17.0 x 28.4in) • Weight: <ul style="list-style-type: none"> • nShield 5c: 11.5kg (25.4lb) • nShield 5c 10G: 12kg (26.5 lbs) • Input voltage: 100-240V AC auto switching 50-60Hz • Power consumption: 220W (Maximum) • Heat dissipation: <ul style="list-style-type: none"> • nShield 5c: 445 BTU/hr (typical load) • nShield 5c 10G: 307 BTU/hr (typical load) • Reliability – MTBF³: <ul style="list-style-type: none"> • nShield 5c: 107,845 hours • nShield 5c 10G: 137,668 hours

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