![Entrust logo]

# Entrust nShield® 5c HSMs

High-performance, 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.

- High cryptographic transaction rates and flexible scaling

- Integrate with over 150 leading application provider solutions

- Powerful remote configuration and management capability following simple installation

- Integration with **Entrust KeyControl for key & secrets management** throughout their lifecycle

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 telecom

- IoT applications

- Car2X

**Learn more at entrust.com/HSM**

# nShield 5c HSMs

## KEY FEATURES & BENEFITS
### 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 5s 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 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 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.

**Key and Secrets Management** – nShield 5 can be integrated with Entrust KeyControl. The nShield 5 HSM is used to protect the master key for the KeyControl virtual appliance and in the process of generating high-quality cryptographic keys using a hardware-based random number generator.

# nShield 5c HSMs

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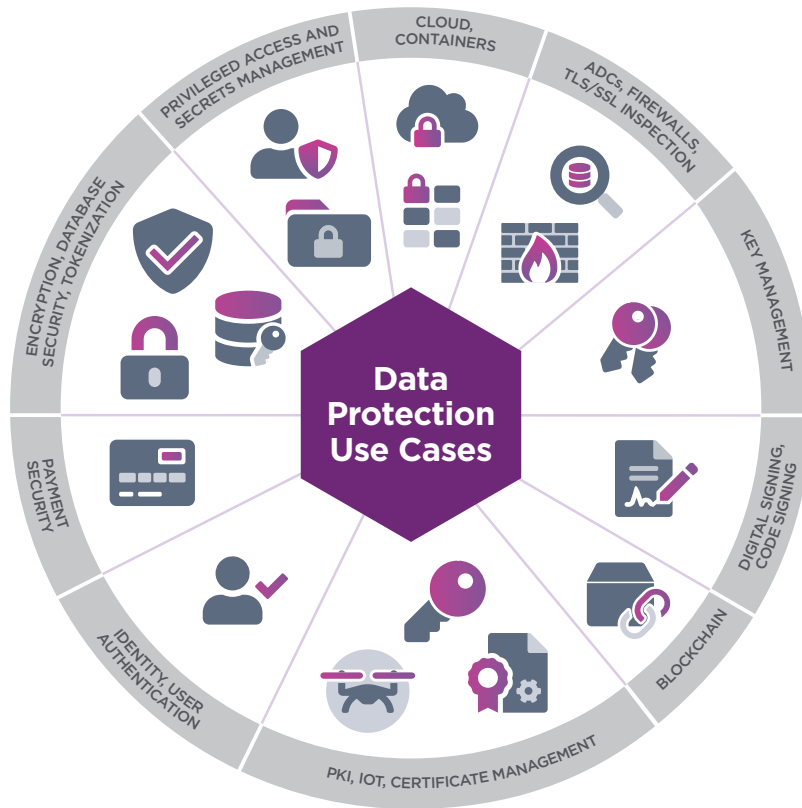


## AVAILABLE MODELS AND PERFORMANCE

| nShield 5c 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 |
| 521 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)** | | | |
| ECDH P-256 bit | 2,085 | 7,550 | 21,436 |
| **Client licenses** | | | |
| Included | 3 | 3 | 3 |
| Maximum | 10 | 20 | unlimited[1] |

Note 1: Requires enterprise client license.

# nShield 5c HSMs

## TECHNICAL SPECIFICATIONS

| Supported cryptographic algorithms | Supported platforms | Application programming interfaces (APIs) | Host connectivity | Security compliance |
|---|---|---|---|---|
| • Full NIST Suite B implementation<br><br>• Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA (including NIST, Brainpool & secp256k1 curves), ECDH, Edwards (Ed25519, Ed25519ph<br><br>• 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<br><br>• Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160, SHA-3 (224, 256, 384, 512 bit)<br><br>• Elliptic Curve Key Agreement (ECKA) available via Java API and nCore APIs<br><br>• Elliptic Curve Integrated Encryption Scheme (ECIES) available via Java API, PKCS#11 and nCore APIs<br><br>• TUAK and MILENAGE algorithm support for mutual authentication and key generation (3GPP)<br><br>• NIST short-listed post-quantum cryptographic algorithms supported using the nShield 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 | • PKCS#11<br>• OpenSSL<br>• Java (JCE)<br>• Microsoft CAPI/CNG<br>• Web Services<br>• nCore | • Dual Gigabit Ethernet ports (two network segments with network bonding option) | • FIPS 140-3 Level 3<br>• BSI AIS 20/31 compliant<br>• eIDAS and Common Criteria EAL4+ |

| Safety, EMC & environmental compliance | High availability | Management and monitoring | Physical characteristics |
|---|---|---|---|
| • UL, CE, FCC, UKCA, RCM, Canada ICES<br><br>• RoHS, WEEE, REACH | • All solid-state storage<br><br>• Field serviceable fan tray<br><br>• Dual hot-swap power supplies<br><br>• Full support for clustering HSMs and automated failover/load balancing<br><br>• Network bonding supporting active backup mode and 802.3ad mode | • KeySafe 5, nShield Remote Configuration<br><br>• nShield Remote Administration (purchased separately)<br><br>• Secure audit logging<br><br>• Syslog diagnostics support and Windows performance monitoring<br><br>• SNMP monitoring agent | • Standard 1U 19in. rack mount<br><br>• Dimensions: 43.4 x 430 x 705mm (1.7 x 16.9 x 27.8in)<br><br>• Weight: 11.5kg (25.4lb)<br><br>• Input voltage: 100-240V AC auto switching 50-60Hz<br><br>• Power consumption: up to 2.0A at 110V AC, 60Hz \| 1.0A at 220V AC, 50Hz<br><br>• Heat dissipation: 327.6 to 362.0 BTU/hr (full load)<br><br>• Reliability – MTBF[2]: 107,845 hours |

Note 2: 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**