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 (pending) 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

nShield 5c HSMs are tamper-resistant appliances 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 5c HSMs support high transaction rates, making them ideal for enterprise application environments where throughput is critical, such as 5G, Car2X, and smart meters.

Centralized remote management

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

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.

nShield Monitor – Provides a single dashboard of all your nShield HSMs, helping you to optimize operations and increase uptime. Separate data sheet available.

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 • 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) • NIST short-listed post-quantum cryptographic algorithms supported using the nShield Post Quantum SDK with CodeSafe	• 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 • OpenSSL • Java (JCE) • Microsoft CAPI/CNG • Web Services • nCore	• Dual Gigabit Ethernet ports (two network segments with network bonding option)	• FIPS 140-3 Level 3 (pending) • BSI AIS 20/31 compliant

Safety, EMC & environmental compliance	High availability	Management and monitoring	Physical characteristics
• UL, CE, FCC, UKCA, RCM, Canada ICES • RoHS, WEEE, REACH	• 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	• KeySafe 5, nShield Remote Configuration • nShield Remote Administration (purchased separately) • nShield Monitor (purchased separately) • Secure audit logging • Syslog diagnostics support and Windows performance monitoring • SNMP monitoring agent	• Standard 1U 19in. rack mount • Dimensions: 43.4 x 430 x 705mm (1.7 x 16.9 x 27.8in) • Weight: 11.5kg (25.4lb) • Input voltage: 100-240V AC auto switching 50-60Hz • Power consumption: up to 2.0A at 110V AC, 60Hz | 1.0A at 220V AC, 50Hz • Heat dissipation: 327.6 to 362.0 BTU/hr (full load) • 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

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data. 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