DATA SHEET

Entrust nShield® Connect HSMs

The security of your applications depends on where you keep your keys.

HIGHLIGHTS

Comprehensive Capabilities

Entrust nShield® Connect Hardware Security Modules (HSMs) are FIPS 140-2 Level 3 and Common Criteria EAL4+ (EN 419 221-5) certified appliances that deliver scalable and highly available cryptographic key services across networks.

- Prepare for a post-quantum future with PQC algorithm support
- Integrate with over 150 leading application provider solutions
- CodeSafe option for protecting your application and business logic within the nShield HSM's secure execution environment
- Cloud Disaster Recovery (CDR) option enables convenient and cost-effective way to add off-site failover cryptographic resources to increase redundancy and reliability across any nShield as a Service region
- Integration with Entrust **Cryptographic Security Platform** provides root of trust for key and secrets management, PKI, and certificate lifecycle management

nShield Connect HSMs are tamper-resistant platforms that support key generation and strong protection when not in use. They provide a secure environment for cryptographic functions such as encryption and digital signing for an extensive range of applications, such as:

- Certificate authorities
- Code signing
- Custom software
- Cloud and containerized applications
- Web services
- Remote signing
- Blockchain
- Database encryption

ENTRUST
SECURING A WORLD IN MOTION

KEY FEATURES & BENEFITS

Post-Quantum Support

nShield Connect HSMs support NIST-standardized quantum-resistant algorithms, paving the way for resilient security in the post-quantum era.

Highly Flexible Architecture

Our 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.

Central Management, Configuration, and Monitoring

The 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.

Process More Data Faster

nShield Connect HSMs support high transaction rates, making them ideal for environments where throughput is critical, such as enterprise, retail, and IoT.

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 version of Connect XC 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.

Protect Your Proprietary Applications

The CodeSafe option provides a secure environment for running sensitive applications within nShield FIPS 140-2 Level 3 physical boundary.

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[3]			
256 bit	680	7,515[2]	14,400[2]
Symmetric encryption (KB/sec) 1024 byte plain text			
AES 128 bit	825	7,700	11,300
AES 256 bit	795	7,700	9,700
Key generation (keys/sec)			
RSA 2048 bit	6.0	6.2	7.3
ECDSA P-192 bit[3]	110	650	1,050
ECDSA P-256 bit[3]	100	630	1,050
ECDSA P-521 bit[3]	65	480	710
Client licenses			
Included	3	3	3
Maximum	10	20	unlimited[1]

1: Requires enterprise client license.
2: Performance indicated requires ECDSA fast RNG feature activation available free of charge on request from Entrust nShield Support.
3: Requires ECC activation

Technical Specifications

Supported cryptographic algorithms	Supported platforms	Application programming interfaces (APIs)	Host connectivity	Security compliance
• 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, 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, 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 algorithm support for mutual authentication and key generation (3GPP) • LMS and additional PQC algorithm support (requires CodeSafe/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 • OpenSSL • Java (JCE) • Microsoft CAPI/ CNG • Web Services (requires Web Services Option Pack) • nCore	• Dual Gigabit Ethernet ports (two network segments with network bonding option)	• FIPS 140-2 Level 2 and Level 3 certified • IPv6 certified and USGv6 Ready compliant • 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 • Recognized as a Type 1 QSCD; Type 2 QSCD together with Entrust SAM • BSI AIS 20/31 compliant

Technical Specifications

Safety, EMC & Environmental Compliance	High availability	Management and monitoring	Physical characteristics
• UL, CE, FCC, UKCA, RCM, Canada ICES, RoHS, WEEE	• 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	• nShield Remote Configuration (available on Serial Console-configured models) • nShield Remote Administration (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 (hours)[4], Connect XC: 107,384 hours

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

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION