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.

- High cryptographic transaction rates and flexible scaling

- 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

nShield Connect HSMs are tamper-resistant platforms that perform such functions as encryption, digital signing, and key generation and protection over a range of applications, such as:

- Certificate authorities

- Code signing

- Custom software

- Cloud and containerized applications

- Web services

- Remote signing

- Blockchain

- Database encryption

nShield Connect HSMs

KEY FEATURES & BENEFITS

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.

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.

POWERFUL REMOTE FEATURE 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 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.

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

Protect your proprietary applications

The CodeSafe option provides a secure environment for running sensitive applications within nShield FIPS 140-2 Level 3 physical boundary. Reference the CodeSafe data sheet for more detailed information.

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			
256 bit	680	7,515[2]	14,400[2]
Symmetric encryption (KB/sec) 1024 byte plain text			
3 DES 168 bit	685	5,140	5,500
AES 128 bit	825	7,700	11,300
Key generation with ECC activation (keys/sec)			
RSA 2048 bit	6.0	6.2	7.3
ECDSA P-192 bit	110	650	1,050
ECDSA P-256 bit	100	630	1,050
ECDSA P-521 bit	65	480	710
Client licenses			
Included	3	3	3
Maximum	10	20	unlimited[1]

Note 1: Requires enterprise client license.

Note 2: Performance indicated requires ECDSA fast RNG feature activation available free of charge on request from Entrust nShield Support.

nShield Connect 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, 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 • 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	• Windows and Linux operating systems including distributions from RedHat, 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)	• 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 Qualified Signature Creation Device • BSI AIS 20/31 compliant

Safety and environmental standards compliance	High availability	Management and monitoring	Physical characteristics
• UL, CE, FCC, RCM, Canada ICES, RoHS2, WEEE	• All solid-state storage • Field serviceable fan tray • Dual hot-swap power supplies • Full support for clustering HSMs and automated failover/ load balancing	• nShield Remote Configuration (available on Serial Console-configured models) • 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 (hours)[3], Connect XC: 107,384 hours

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

To find out more about
Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 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/HSM

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
HSMinfo@entrust.com