NCIPHER

www.ncipher.com

nShield Connect

- Maximizes performance and availability with high cryptographic transaction rates and flexible scaling
- Supports a wide variety of applications including certificate authorities, code signing and more
- nShield CodeSafe protects your applications and business logic within nShield's secure execution environment
- nShield Remote Administration, Configuration and Monitor options help reduce travel and manage HSMs more efficiently

nShield Connect HSMs

Certified appliances that deliver scalable and highly available cryptographic key services across networks

nShield Connect HSMs

Feature Overview

nShield Connect HSMs are FIPS-certified appliances that deliver cryptographic services to applications across the network. These tamper-resistant platforms perform such functions as encryption, digital signing and key generation and protection over an extensive range of applications, including certificate authorities, code signing, custom software and more.

The nShield Connect series includes nShield Connect+ and the new, high-performance nShield Connect XC.

HIGHLY FLEXIBLE ARCHITECTURE

nCipher's 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 enterprise, retail, IoT and other environments where throughput is critical.

PROTECT YOUR PROPRIETARY APPLICATIONS

The CodeSafe option provides a secure environment for running sensitive applications within nShield boundaries.

TECHNICAL SPECIFICATIONS

Supported cryptographic algorithms

- 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, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, Triple DES
- Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160
- Full Suite B implementation with fully licensed ECC, including Brainpool and custom curves

Supported operating systems

- Microsoft Windows 7 x64, 10 x64; Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- Red Hat Enterprise Linux AS/ES 6 x64, 6 x86, 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
- Oracle Solaris 11 (SPARC), Oracle Solaris 11 x64
- IBM AIX 7.1 (POWER6, POWER8), HP-UX 11i v3
- Oracle Enterprise Linux 6.8 x64 and 7.1 x64

Application programming interfaces (APIs)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore, nShield Web Services Crypto API

Host connectivity

- Dual Gigabit Ethernet ports (two network segments)

Security compliance

- FIPS 140-2 Level 2 and Level 3 certified
- IPv6 certified and USGv6 Ready compliant
- Connect+: Common Criteria EAL4+ (AVA_VAN.5) certified
- Connect+ recognized as a Qualified Signature Creation Device
- Connect XC: BSI AIS 20/31 compliant

Safety and environmental standards compliance

- UL, CE, FCC, C-TICK, Canada ICES RoHS2, WEEE

High availability

- All solid-state storage
- Field serviceable components, dual hot-swap power supplies

Management and monitoring

- nShield Remote Configuration (available on Serial Console-configured Connect XC models)
- nShield Remote Administration (purchased separately)
- nShield Monitor (purchased separately)
- Secure audit logging
- Syslog diagnostics support and Windows performance monitoring
- SNMP monitoring agent

Physical characteristics

- 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)

AVAILABLE MODELS AND PERFORMANCE

nShield Connect Models	500+	XC Base	1500+	6000+	XC Mid	XC High
RSA Signing Performance (tps) for NIST Recommended Key Lengths						
2048 bit	150	430	450	3,000	3,500	8,600
4096 bit	80	100	190	500	850	2,025
ECC Prime Curve Signing Performance (tps) for NIST Recommended Key Lengths						
256 bit	540	680	1,260	2,400	5,500	14,400
Client Licenses						
Included	3	3	3	3	3	3
Maximum	10	10	20	100	20	100

LEARN MORE

To find out more how nCipher Security can deliver trust, integrity and control to your business critical information and applications, visit ncipher.com

Search: nCipherSecurity

www.ncipher.com

nCIPHER