THALES

www.thales-esecurity.com

NETWORK-ATTACHED HARDWARE SECURITY MODULES

The Thales nShield Connect series are network attached hardware security modules (HSMs) that increase the digital security of an organization's critical business applications by isolating sensitive tasks, securely executing cryptographic operations, and protecting and managing the associated keys. These hardened, tamper-resistant platforms perform encryption, digital signing and key management on behalf of an extensive range of commercial and custom-built applications including public key infrastructures (PKIs), identity management systems, application-level encryption and tokenization, SSL/TLS, and code signing. High assurance alternatives to the software-based cryptography libraries, nShield Connect modules feature certified implementations of all leading algorithms including Suite B, as well as best in class elliptic curve cryptography (ECC) performance.

▷ **Key Benefits**

- Automate risk-prone administrative tasks, guarantee key recovery, and eliminate costly manually-intensive backup processes
- Remote Administration feature reduces the cost of traveling to data centers
- Establish strong separation of duties through robust administration policies including roles-based multi-factor authentication and quorum-based authorization
- Enable secure execution of custom security-critical application code within the tamper-resistant hardware boundary

Thales e-Security

nShield Connect Series

Connect+ and Connect XC

Thales nShield Connect Series

TECHNICAL SPECIFICATIONS[1]

Functional capabilities
- Secure key and application storage and processing
- Cryptographic offloading and acceleration
- Authenticated multi level access control
- Strong separation of administration and operator roles
- Hardened client authentication using nToken hardware
- Secure key wrapping, backup, replication and recovery
- Unlimited protected key storage
- Supports clustering and load-balancing
- Logical cryptographic separation of application keys
- "k of n" multi-factor authentication

Supported operating systems
- Windows, Linux, Solaris[4], IBM AIX[4], HP – UX[4]
- Server side: Windows, Linux, Solaris, IBM AIX, HP-UX
- Supports numerous VM software vendors including VMware, Hyper-V and AIX LPARs
- Remote Administration client side: Windows, Linux

Application Program Interfaces (APIs)
- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG
- nCore (low-level Thales interface for developers)

Compatibility and upgradeability
- Compatible with Thales nShield Connect, nShield Solo PCI/PCIe/ PCIe+ and nShield Edge
- Security World key management architecture enables load balancing across mixed estates of nShield models
- Software upgradeable

Host connectivity
- Dual Gigabit Ethernet ports (services two network segments)

Cryptography
- Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA[3], ECDH[3]
- Symmetric algorithms: AES, ARIA, Camellia, CAST, RIPEMD160 HMAC, SEED, Triple DES
- Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit)
- Full Suite B implementation with fully licensed ECC including Brainpool and custom curves

Security[2] compliance
- FIPS 140-2 Level 2 and Level 3 (XC models FIPS-pending)

Safety and enviromental compliance
- UL, CE, FCC, C-TICK, and Canada ICES
- RoHS2, WEEE

High availability
- All solid-state storage
- Dual hot-swap power supplies
- Field serviceable components (power supplies and fans)

Management and monitoring
- Remote Administration enables management—including adding applications, updating firmware, and checking nShield status—from your office location
- Syslog diagnostics support
- Windows performance monitoring
- Command line interface (CLI)/graphical user interface (GUI)
- SNMP monitoring agent

Physical characteristics
- Standard 1U 19in. rack mount with integrated Smart Card Reader
- 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 (nominal)/ IEC 320 mains socket and rocker switch
- Power consumption: up to 1.2A at 110v AC 60Hz or 0.6A 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	340	450	3,000	3,000	8,400
4096 bit	80	80	190	500	700	2,000
ECC Prime Curve Signing Performance (tps) for NIST Recommended Key Lengths[3]						
256 bit	540	570	1,260	2,400	5,000	14,000

Microsoft Partner
Gold Application Development

1 Performance may vary depending on operating system, application, network topology and other factors.
2 Security certifications are performed only against select firmware versions. Consult the certifications section of our website for links to official certificates.
3 With ECC Activation
4 Connect+ models only

Follow us on:

Americas – Thales e-Security Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel: +44 (0)1844 201800 • Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com