THALES

www.thales-esecurity.com

NETWORK-ATTACHED HARDWARE SECURITY MODULE

The Thales nShield Connect+ is a hardware security module (HSM) that isolates and secures cryptographic operations and associated keys for an organization's most critical applications. This hardened, tamper-resistant platform performs 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. A high assurance alternative to software-based cryptography libraries, nShield Connect+ features certified implementations of all leading algorithms, as well as the world's fastest ECC performance.

Key Benefits

- Automates burdensome and risk-prone administrative tasks, guarantees key recovery, and eliminates single points of failure and expensive, manually-intensive backup processes
- Establishes strong separation of duties and dual controls through robust administration policies including role-based multi-factor authentication and flexible quorum-based authorization
- Enables secure execution of custom security-critical application code within the tamper-resistant hardware boundary

Thales e-Security

nShield Connect+

Thales nShield Connect+

TECHNICAL SPECIFICATIONS*

Functional capabilities
- Onboard secure key and application storage/processing
- Cryptographic offloading/acceleration
- Authenticated multi level access control
- Strong separation of duties (administrator and operator)
- nToken option provides unmatched client authentication
- Secure key wrapping, backup, replication and recovery
- Unlimited protected key storage
- Clustering, load-balancing and "k of n" multifactor authentication
- Unlimited logical/cryptographic separation of application keys

Supported operating systems
- Physical: Windows, Linux, Solaris, IBM AIX, HP-UX
- Virtual: supports numerous VM software vendors including VMware, Hyper-V and AIX LPARs

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

Scalability, compatibility and upgradeability
- Up to 100 clients
- Compatible with Thales nShield Connect, nShield Solo PCI/ PCIe/PCIe+ and nShield Edge
- Software upgradeable

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

Cryptography
- A symmetric public key algorithms: RSA (1024, 2048, 4096), Diffie-Hellman, DSA, El-Gamal, KCDSA, ECDSA, ECDH
- Symmetric algorithms: AES, ARIA, Camellia, CAST, DES, RIPEMD160 HMAC, SEED, Triple DES
- Hash/message digest: SHA-1, SHA-2 (224, 256, 384, 512 bit)
- Full Suite B implementation with fully licensed Elliptic Curve Cryptography (ECC) including Brainpool and custom curves

Safety, security and environmental compliance
- UL, CE, FCC
- RoHS, WEEE
- FIPS 140-2 Level 2 and Level 3, NIST SP 800-131A

High availability
- All solid-state storage
- Dual hot-swap power supplies
- Field serviceable components (power supplies and fans)
- 47,000 hrs MTBF (Mil-Std 217F notice 2 parts count method)

Management and monitoring
- Remote unattended operator/multi-user access control
- Syslog diagnostics support
- Windows performance monitoring
- Command line interface (CLI)/graphical user interface (GUI)
- SNMPv3 compatible monitoring

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)
- Temperature: operating 5 to 40°C (41 to 104°F), storage -20 to 70°C (-4 to 158°F)
- Humidity: operating 10 to 90% (relative, non-condensing at 35%), storage 0 to 85% (relative, non-condensing at 35%)

Available models and performance

Connect+	500+	1500+	6000+
RSA Signing Performance (tps) for NIST Recommended Key Lengths			
2048 bit	150	450	3000
4096 bit	80	190	500
ECC Prime Curve Signing Performance (tps) for NIST Recommended Key Lengths[Δ]			
192 bit	880	1600	2300
256 bit	540	1260	2400
521 bit	120	330	1300
ECC Key Generation Performance (keys/sec) for NIST Recommended Key Lengths[Δ]			
192 bit	390	445	825
256 bit	250	260	840
521 bit	60	160	480
Client Licenses			
Included	3	3	3
Maximum	10	20	100

[Δ]With ECC Activation

500+ and 1500+ models are available starting July 1, 2014.

Microsoft Partner
Gold Application Development

* Performance may vary depending on operating system, application, network topology and other factors.

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 – Unit 4101, 41/F, 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