THALES

# > Hardware Security Module

## Thales nShield Connect

## KEY BENEFITS

### OPERATIONAL

> Provides unmatched operational flexibility, high availability and scalability in virtualized and cloud environments leveraging unique Security World architecture

> Reduces overall cost for regulatory compliance (e.g. PCI DSS) as well as for day-to-day key management tasks including backup and remote management

> Enables high assurance business continuity with simplified HSM enrollment, efficient key provisioning and fully resilient hardware features including dual hot-swap power supplies and field-serviceable redundant fans

### SECURITY

> Delivers certified protection for cryptographic keys and operations within tamper-resistant hardware to significantly enhance security for critical applications

> 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 hardware security boundary

Microsoft GOLD CERTIFIED Partner ISV

ORACLE CERTIFIED PARTNER

The nShield Connect is the premier network-attached hardware security module (HSM) in the Thales family of high security data protection solutions. The hardened platform, including a model optimized for elliptic curve cryptography, safeguards and manages sensitive keys used for encryption and digital signing on behalf of a wide range of commercial and custom-built business applications. nShield Connect protects critical security systems including public key infrastructures (PKIs), identity management, databases, web fabric, domain name system security extension (DNSSEC) deployments and code signing.

The nShield Connect is the most cost-effective way to establish the appropriate levels of physical and logical controls for server-based systems where software-based security features are considered to be inadequate. In the face of evolving compliance requirements and general standards of due care, the use of nShield HSMs provides a tangible measure of security within the traditional data center, virtualized environments and for cloud-based services. All Thales nShield HSMs feature the market-leading Security World key management architecture that enables the automation of burdensome and risk-prone administrative tasks, guarantees key recovery and eliminates single points of failure and expensive, manually-intensive backup processes.

# > 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 Solo (PCI/PCIe), nShield Edge and netHSM
- Software upgradeable

### Host Connectivity

- Dual Gigabit Ethernet ports (services two network segments)

### Cryptography

- Asymmetric 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, 512bit)
- 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**
- Common Criteria EAL4+**

### 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%)

### Business Continuity

All solid-state memory designed for business continuity, nShield Connect also includes dual, hot-swap power supplies and a field-serviceable fan tray enabling onsite repairs. To further increase availability, several HSMs can be combined for load balancing and fail-over. SNMP support enables remote monitoring of power supplies, temperature, fan speeds and other parameters.

nShield Connect includes dual, hot-swap power supplies, field-serviceable fan trays and optional slide rails for rack mounting.

### Available Models and Performance

nShield Connect is available in four different variants:

| Model | 500 | 1500 | 6000 |
|---|---|---|---|
| Signing Performance RSA (tps) | | | |
| 1024bit | 500 | 1500 | 6000 |
| 2048bit | 150 | 500 | 3000 |
| 4096bit | 65 | 165 | 500 |
| Client Licenses | | | |
| Included | 3 | 3 | 3 |
| Max. | 10 | 20 | 100 |

| Model | 6000+ |
|---|---|
| Signing Performance ECC NISTP (tps) | |
| 192bit | 2300 |
| 256bit | 2400 |
| 521bit | 1300 |
| Client Licenses | |
| Included | 3 |
| Max. | 100 |

For more information please see www.thales-esecurity.com or scan the quick response (QR) code on your smart phone.

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

** Model 6000+ under FIPS and Common Criteria evaluation.





**Americas:** 900 South Pine Island Road, Suite 710, Plantation, Florida 33324 • 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