



> Thales nShield Connect

KEY BENEFITS

- > Enhances security for critical applications
- > Reduces cost of compliance
- > Simplifies encryption and signing key management
- > CodeSafe option enables secure execution of custom applications within the security boundary
- > Helps ensure business continuity and minimize downtime with unique dual power supplies and redundant fans
- > Compatible with other Thales HSMs
- > Offers exceptional scalability with unsurpassed performance for up to 100 clients
- > Delivers FIPS and Common Criteria

Network-attached hardware security module

Thales nShield Connect, part of the nCipher product line, is a network-attached hardware security module (HSM) that protects up to 100 clients by safeguarding their encryption and digital signing keys and processing sensitive data on the trusted appliance. Its unique dual, hot-swap power supplies and redundant, field-replaceable fans make nShield Connect fault tolerant. Providing high availability, scalability and remote management, it enables organizations to build reliable, future-proof cryptographic services. Its security boundary is validated for FIPS 140-2 Level 3 and Common Criteria EAL4+.



>> Thales nShield Connect

Hardware security for applications

nShield Connect enables enterprises to add hardware protection to critical systems such as public key infrastructures (PKIs), databases, web and application servers. Using standard cryptographic interfaces, nShield Connect integrates readily with Microsoft Certificate Services (PKI), Entrust Authority Security Manager, RSA Certificate Manager, Oracle Database, Microsoft SQL Server, and many other applications.

nShield Connect features tamper-responsive, rack-mountable hardware, which generates application keys in a secure hardware boundary. The CodeSafe option enables secure execution of custom applications within the security boundary to protect against insider and Trojan attacks.

Business continuity

Designed for business continuity, nShield Connect is the world's only HSM with dual, hot-swap power supplies and a field-serviceable fan tray, avoiding round-trips to a service center for 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 is the world's only HSM with dual, hot-swap power supplies

Central key management

The Security World management software centrally manages nShield Connect and other nCipher product line HSMs to reduce setup and administration time. Security World securely supports remote operation of HSMs in lights-out data centers, disaster recovery even for total hardware replacements, and key sharing across HSMs and geographies. Keys and meta information can be securely backed up online without requiring additional hardware as the system grows, reducing the total cost of operations.

Scalability and Flexibility

To provide services for up to 100 clients, nShield Connect offers hardware acceleration for cryptographic operations, making it the world's fastest network-attached HSM with up to 6,000 signing transactions per second (TPS) with 1,024 RSA keys.* Using RSA 2,048 bit keys, nShield Connect excels at up to 3,000 TPS.*

nShield Connect integrates with applications through standard interfaces including PKCS#11, OpenSSL, Java Cryptography Extension (JCE), Microsoft CAPI and CNG. It is compatible with nShield Solo (nShield PCI/PCIe) and netHSM and can be upgraded to support additional features using a range of option packs. nShield Connect supports a broad range of operating systems, including Windows 2008/2003/Vista/XP, Linux, Solaris, AIX, and HP-UX. Two Gigabit Ethernet ports enable the HSM to service two network segments.

Cryptography and compliance

nShield Connect supports a broad range of public-key and symmetric algorithms, including a full Suite B implementation with optional, fully licensed elliptic curve cryptography (ECC). nShield Connect's key management is validated to FIPS 140-2 Level 3 and Common Criteria EAL 4+. Following a security best practice and to enable compliance, it provides separation of duties with two-factor authentication and dual control. Organizations can segregate access by application, division, or geography.

Available models

nShield Connect is available in three different variants:

Model number	500	1500	6000
Power supplies	2	2	2
Speed (TPS RSA 1,024)*	500	1500	6000
Speed (TPS RSA 2,048)*	150	500	3000
Incl. client licenses	3	3	3
Max. no. of clients	10	20	100
Front Panel	Black	Black	Silver

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

For more information, please see www.thalesgroup.com/iss.

Thales - Information Systems Security



Certificate no. EMS 73838

Certificate no. FS69836