> Thales nShield Connect 6000

KEY BENEFITS

- > Enhances security for critical applications
- > Reduces cost of compliance
- > Simplifies encryption and signing key management
- > Protects sensitive data by processing it on secure hardware
- > Helps ensure business continuity and minimize downtime with unique dual, hot-swap power supplies and redundant, field-serviceable fans
- > Compatible with Thales nShield and Thales netHSM
- > Offers exceptional scalability with unsurpassed performance for up to 100 clients
- > Delivers FIPS and Common Criteria

Network-attached hardware security module

Thales nShield Connect 6000, part of the nCipher product line, is a network-attached, general-purpose 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 6000 fault tolerant. Providing high availability, scalability and remote management, it enables organizations to build reliable, future-proof cryptographic services. Its key management is validated for FIPS 140-2 Level 3 and Common Criteria EAL4+.

www.thalesgroup.com/iss

>> Thales nShield Connect 6000

Hardware security for applications

nShield Connect 6000 enables enterprises to add hardware protection to critical applications such as public key infrastructures (PKIs), databases, web and application servers. Using standard cryptographic interfaces, nShield Connect 6000 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 6000 features tamper-responsive, rack-mountable hardware with optional slide rails. Secure code execution for sensitive data processing on the HSM platform protects against insider and Trojan attacks. nToken adds client hardware authentication.

Availability

Designed for business continuity, nShield Connect 6000 is the world's only general-purpose HSM with dual, hot-swap power supplies. The redundant fans can be replaced without sending the unit to a service center. To further increase availability, several HSMs can be clustered and load balanced.

nShield Connect 6000 is the world's only general-purpose HSM with dual, hot-swap power supplies

Management

The Security World management software centrally manages nShield Connect 6000, nShield and netHSM 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 automatically backed up without requiring additional hardware as the system, reducing the total cost of operations.

Scalability and Flexibility

To provide services for up to 100 clients, nShield Connect 6000 offers hardware acceleration for cryptographic operations, making it the world's fastest network-attached HSMs with up to 6,000 signing transactions per second (TPS) with 1,024 RSA keys. Using RSA 2,048 bit keys, nShield Connect 6000 excels at up to 3,000*. Web servers, such as Microsoft IIS and Apache, can increase SSL throughput by off-loading handshakes operations to the nShield 6000.

nShield Connect 6000 integrates with applications through standard interfaces including PKCS#11, Java Cryptography Extension (JCE), Microsoft CAPI and CNG. It is compatible with other Thales nShield and Thales netHSM products and can be upgraded to support additional features using various Option Packs. nShield Connect 6000 supports a broad range of operating systems, including Windows 2008/2003/Vista/XP, Linux Solaris, AIX and HPUX. Two Gigabit Ethernet ports enable the HSM to service two network segments.

Cryptography and compliance

nShield Connect 6000 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 6000's key management is validated to FIPS 140-2 Level 3 and Common Criteria EAL 4+. Following security best practice and to enable compliance, it separates administrative and operational duties with two-factor authentication and multiple-person control (k of n). These operator groups can segregate access to keys by application, role, division, or geography.

Integrated services

Thales offers professional services to ensure a best practice implementation of Thales HSMs. Organizations can benefit from developer support to integrate Thales HSMs with custom applications or to develop custom applications to be executed on the HSM to process sensitive data.

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

For more information, please see www.thales-group.com/iss.

Certificate no. EMS 73838

Certificate no. FS69836

Thales - Information Systems Security

Americas: 2200 North Commerce Parkway, Suite 200, Weston, Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road Central, Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Australia: Level 2, 103-105 Northbourne Avenue, Turner, ACT 2601, Australia • Tel: +61 2 6120 5186 • Fax: +61 2 6120 5101 • E-mail: sales.australasia@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