THALES

www.thales-esecurity.com

PORTABLE HARDWARE SECURITY MODULE

The Thales nShield Edge is a full-featured portable hardware security module (HSM) that increases 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. Designed for low transaction volume environments, this USB-connected device performs encryption, digital signing and key management on behalf of an extensive range of commercial and custom-built applications including offline certificate authorities (CAs) and code signing. A high assurance alternative to software-based cryptography libraries, nShield Edge features certified implementations of all leading algorithms including Suite B.

▷ **Key Benefits**

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

Thales e-Security

nShield Edge

Thales nShield Edge

TECHNICAL SPECIFICATIONS*

Functional capabilities
- Protects cryptographic keys in secure hardware
- Supports laptops and virtual machines
- Strong separation of administration and operator roles
- Protects keys for registration authorities
- Facilitates remote nShield HSM operation
- Simplifies HSM application development
- Provides secure key wrapping, backup, replication and recovery
- Supports unlimited protected key storage and logical/ cryptographic separation of application keys
- "k of n" multifactor authentication

Supported operating systems
- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 R2, Windows 7
- VMware Server, VMware Workstation, Hyper-V for Windows Server 2008 R2, MS Virtual PC for Windows 7

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/Connect+ and nShield Solo PCI/PCIe/PCIe+
- Security World key management architecture enables load balancing across mixed estates of nShield models

Host connectivity
- USB port (1.x, 2.x compliant)
- Includes 1 meter connector cable (USB type A to B)

Cryptography
- Asymmetric public key algorithms: RSA, Diffie-Hellman, DSA, KCDSA, ECDSA, ECDH
- 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 Elliptic Curve Cryptography (ECC) including Brainpool and custom curves

Security** compliance
- FIPS 140-2 Level 2 and Level 3, and NIST SP 800-131A

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

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 agent

Physical characteristics
- Portable desktop device with integrated smart card reader
- Dimensions with stand open 120 x 118 x 27mm (4.7 x 4.6 x 1in)
- Weight: 340g (0.8lb)
- Input voltage: 5v DC powered by USB host device
- Power consumption: 700mW
- Temperature: operating 5 to 45°C (41 to 113°F), storage -40 to 70°C (-40 to 158°F)
- Humidity: operating 10 to 90% (relative, non-condensing), storage 0 to 95% (relative, non-condensing)

Available models and performance
- nShield Edge is available in FIPS Level 2 and Level 3 variants
- A non-FIPS Developer Edition is also available
- Signing performance for NIST recommended key lengths
  - 2048 bit RSA: 2 tps
  - 4096 bit RSA: 0.2 tps

Microsoft Partner
Gold Application Development

* Performance may vary depending on operating system, application, network topology and other factors.
** Security certifications are performed only against select firmware versions. Consult the certifications section of our website for links to official certificates.

© Thales - October 2015 • PLB5122

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