THALES

www.thalesesecurity.com

nSHIELD EDGE

- Maximizes cost efficiency. nShield Edge is the most economical HSM in the nShield family
- Supports a wide variety of applications including certificate authorities, code signing and more
- Delivers strong security. nShield Edge HSMs are certified up to FIPS 140-2 Level 3

‹Thales eSecurity›

nSHIELD EDGE HSMs

Certified USB-connected Devices that Deliver Cryptographic Key Services to Desktop Applications

‹Thales eSecurity›

nSHIELD EDGE HSMs

Feature Overview

nShield Edge hardware security modules (HSMs) are full-featured, FIPS-certified, USB-connected devices that deliver encryption, key generation and key protection along with convenience and economy.

DESIGNED FOR LOW-VOLUME TRANSACTION ENVIRONMENTS

Suits off-line key generation and development environments, while delivering complete algorithm and API support.

HIGHLY PORTABLE

Small, lightweight design with convenient USB interface supports a variety of platforms, including laptops and other portable devices.

COST EFFECTIVE AND SCALABLE

The most economical HSM in the nShield family, nShield Edge gives you an entry-point HSM, while affording you the option to scale your environment as your needs grow. Thales's unique Security World architecture lets you combine nShield HSM models to build a mixed estate that delivers flexible scalability, key sharing, seamless failover and load balancing.

TECHNICAL SPECIFICATIONS

Supported Cryptographic Algorithms

- Asymmetric algorithms: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)
- Symmetric algorithms: AES, Arcfour, ARIA, Camellia, CAST, DES, MD5 HMAC, RIPEMD160 HMAC, SEED, SHA-1 HMAC, SHA-224 HMAC, SHA-256 HMAC, SHA-384 HMAC, SHA-512 HMAC, Tiger HMAC, Triple DES
- Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160
- Full Suite B implementation with fully licensed ECC, including Brainpool and custom curves

Supported Operating Systems

- Microsoft Windows 7 x64, 10 x64, Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- Red Hat Enterprise Linux AS/ES 6 x64, x86 and 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
- Oracle Enterprise Linux 6.8 x64, 7.1 x64

Application Programming Interfaces (APIs)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore, nShield Web Services Crypto API

Compatibility and Upgradeability

- USB port (1.x, 2.x compliant)

Security Compliance

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

Safety and Environmental Standards Compliance

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

Management and Monitoring

- Remote unattended operator/multi-user access control
- Secure audit logging
- Syslog diagnostics support
- Windows performance monitoring
- SNMP 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

Performance

- Signing performance for NIST recommended key lengths:
- 2048 bit RSA: 2 tps
- 4096 bit RSA: 0.2 tps

AVAILABLE MODELS

- nShield Edge is available in FIPS Level 2 and Level 3 variants
- A non-FIPS Developer Edition is also available

LEARN MORE

Visit us at www.thalesesecurity.com to learn how our advanced data security solutions and services deliver trust wherever information is created, shared or stored.

Follow us on:

Americas – Thales eSecurity 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