THALES

> Hardware Security Module

Thales nShield Edge

KEY BENEFITS

OPERATIONAL

> Provides a portable, cost-effective solution with unmatched operational flexibility for laptops and virtual machines based on the 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 and efficient key provisioning

> Protects registration authority keys and provides a practical solution for offline root CAs

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

Microsoft GOLD CERTIFIED Partner ISV

ORACLE CERTIFIED PARTNER

The nShield Edge is the universal serial bus (USB)-attached hardware security module (HSM) in the Thales family of high security data protection solutions. The nShield Edge combines a full-featured HSM with a smart card reader in one portable device, offering secure backup and dual control access to an organization's high-value keys for low transaction volume environments. The independently certified platform performs key management and cryptographic operations such as encryption and digital signing on behalf of a wide range of commercial and custom-built business applications and critical security systems including offline certificate authorities (CAs) for public key infrastructures (PKIs), code signing and remote HSM management.

The nShield Edge's USB connectivity makes it especially suitable for use with laptops and virtual machines, providing appropriate levels of physical and logical controls 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. 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 Edge

Technical Specifications*

Functional Capabilities

- Protects cryptographic keys in secure hardware
- Supports laptops and virtual machines
- Provides dual control access for valuable keys
- Provides practical solution for offline root CAs
- Protects keys for registration authorities
- Controls keys used for code signing
- 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
- Offers "k of n" multifactor authentication

Supported Operating Systems

- Physical: Windows 2008, 2008 R2, XP, Vista, 7
- Virtual: VMware Server, VMware Workstation, Microsoft 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 Solo (PCI/PCIe), nShield Connect, and netHSM 500 and 2000
- Software upgradeable

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 (1024, 2048, 4096, 8192), 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

High Availability

- All solid-state storage

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

- 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)

Availability and Performance

nShield Edge is available in FIPS Level 3 and Level 2 variants. A non-FIPS Developer Edition is also offered. All modes yield the same performance characteristics.

Signing Performance	(tps)
1024bit RSA	12
2048bit RSA	2
4096bit RSA	0.2

nShield Edge includes smart cards and folds for convenient storage.

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.

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: 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