nShield Edge HSMs

Certified USB-connected devices that deliver cryptographic key services to desktop applications

HIGHLIGHTS

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.

- 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

Designed for low-volume transaction environments

Suits off-line key generation and development environments, while delivering complete algorithm and API support. Ideal for Bring Your Own Key (BYOK) deployments requiring generation of cryptographic keys with FIPS 140-2 level assurance prior to securely exporting them to the cloud.

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. Entrust'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.

LEARN MORE AT ENTRUST.COM/HSM

nShield Edge HSMs

TECHNICAL SPECIFICATIONS

Supported cryptographic algorithms (including full NIST Suite B implementation)	Operating systems	Application programming interfaces (APIs)	Compatibility and upgradeability	Security compliance
• 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, 3DES • Hash/message digest: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bit), HAS-160, RIPEMD160	• Microsoft Windows 7 x64, 10 x64, Windows Server, 2012 R2 x64, 2016 x64, 2019 x64 • Red Hat Enterprise Linux AS/ES 6 x64, x86 and 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64, 15.1 x64 • Oracle Enterprise Linux 6.10 x64, 7.6 x64	• PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI and CNG, nCore, Web Services (requires web services option pack)	• USB port (1.x, 2.x compliant)	• FIPS 140-2 Level 2 and Level 3

Safety and environmental standards compliance	Management and monitoring	Physical characteristics	Performance
• UL, CE, FCC, RCM, and Canada ICES RoHS2, WEEE	• Secure audit logging	• 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	• Signing performance for NIST recommended key lengths: • 2048 bit RSA: 2 tps • 4096 bit RSA: 0.2 tps

AVAILABLE MODELS AND PERFORMANCE

- nShield Edge is available in FIPS Level 2 and Level 3 variants
- A non-FIPS developer edition is also available

Learn more

To find out more about Entrust nShield HSMs visit **entrust.com/HSM**. To learn more about Entrust's digital security solutions for identities, access, communications and data visit **entrust.com**

Learn more at
entrust.com/HSM

ENTRUST

Contact us:
HSMinfo@entrust.com