nShield Edge HSM

Zertifizierte Geräte mit USB-Anschluss, die kryptographische Schlüsseldienste für Desktop-Anwendungen bereitstellen

HIGHLIGHTS

nShield Edge-Hardware-Sicherheitsmodule (HSM) sind voll funktionsfähige, FIPS-zertifizierte Geräte mit USB-Anschluss, die Verschlüsselung, Schlüsselerzeugung und Schlüsselschutz sowie Benutzerfreundlichkeit und Wirtschaftlichkeit bieten.

- Sie sind besonders kosteneffizient: nShield Edge ist das günstigste HSM in der nShield-Familie.
- Sie unterstützen eine Vielzahl an Anwendungen wie Zertifizierungsstellen, Code Signing und mehr.
- Sie liefern hohe Sicherheit. nShield Edge HSM sind bis zu FIPS 140-2 Level 3 zertifiziert.

Für Umgebungen mit geringem Transaktionsvolumen ausgelegt

nShield-HSM eignen sich für Offline-Schlüsselgenerierungs- und Entwicklungsumgebungen und bieten gleichzeitig vollständige Algorithmen- und API-Unterstützung. Sie sind perfekt für Bring-your-own-Key-Bereitstellungen (BYOK), bei denen gewährleistet sein muss, dass die kryptographischen Schlüssel für den sicheren Export in die Cloud gemäß FIPS 140-2 erstellt werden.

Leicht und tragbar

Das USB-HSM ist klein und leicht und verfügt über einen praktischen USB-Anschluss, der eine Vielzahl an Host-Plattformen einschließlich Laptops und sonstige tragbare Geräte unterstützt.

Kostengünstig und skalierbar

nShield Edge, das günstigste HSM der nShield-Reihe, ist das perfekte Einsteigermodell, das Sie jederzeit bei Bedarf skalieren können. Mit der einzigartigen Security-World-Architektur von Entrust kombinieren Sie nShield-HSM-Modelle zu einer gemischten Infrastruktur, die flexible Skalierbarkeit sowie nahtlosen Failover und Lastenausgleich bietet.

WEITERE INFORMATIONEN AUF ENTRUST.COM/HSM

nShield Edge HSM

TECHNISCHE DATEN

Unterstützte kryptographische Algorithmen (einschließlich vollständiger NIST-Suite-B-Implementation)	Betriebssysteme	Anwendungspro-grammier-Schnitt-stellen (APIs)	Kompatibilität und Aufrüstbarkeit	Sicher-heits-Com-pliance:
• Asymmetrische Algorithmen: RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph) • Symmetrische Algorithmen: 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-/Hashwert: MD5, SHA-1, SHA-2 (224, 256, 384, 512 Bit), HAS-160, RIPEMD 160	• Microsoft Windows 7 x64, 10 x64, Windows Server, 2012 R2 x64, 2016 x64, 2019 x64 • RedHat Enterprise Linux AS/ES 6 x64, x86 und 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 und CNG, nCore, Web Services (erfordert das Web Services Option Pack)	• USB-Anschluss (1.x, 2.x-konform)	• FIPS 140-2 Level 2 und Level 3

Einhaltung von Sicherheits- und Umweltstandards	Verwaltung und Überwachung	Physische Eigenschaften	Leistung
• UL, CE, FCC, RCM, und kanadischer ICES RoHS2, WEEE	• Sichere Audit-Protokollierung	• Tragbares Desktop-Gerät mit integriertem Chipkartenleser • Abmessungen mit offenem Ständer 120 x 118 x 27 mm (4,7 x 4,6 x 1in) • Gewicht: 340g (0,8lb) • Eingangsspannung: 5 V DC, gespeist von einem USB-Host-Gerät • Leistungsaufnahme: 700mW	• Signierleistung für die von NIST empfohlenen Schlüssellängen: • 2048 Bit RSA: 2 tps • 4096 Bit RSA: 0,2 tps

VERFÜGBARE MODELLE UND LEISTUNG

- nShield Edge ist in den Varianten FIPS Level 2 und Level 3 erhältlich.
- Zudem wird eine nicht FIPS-zertifizierte Developer Edition angeboten.

Weitere Informationen

Mehr Informationen zu den nShield HSM von Entrust finden Sie auf **entrust.com/HSM**. Auf **entrust.com** erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.

Weitere Informationen auf
entrust.com/HSM

ENTRUST

Kontakt:
HSMinfo@entrust.com