



ENTRUST

Les HSM nShield Edge

Appareils USB certifiés qui fournissent des services de clés chiffrées aux applications de bureau

CARACTÉRISTIQUES

Les modules matériels de sécurité (HSM) nShield Edge sont des appareils complets, certifiés FIPS et reliés par USB qui permettent de chiffrer, de générer et de protéger des, de façon pratique et à moindre coût.

- Optimise le rendement. nShield Edge est le HSM le plus abordable de la gamme nShield
- Prend en charge un large éventail d'applications, telles que les autorités de certification, la signature de code et plus encore
- Assure un haut niveau de protection. Les HSM nShield Edge sont certifiés conformes à la norme FIPS 140-2 niveau 3

Conçu pour les environnements à faible volume de transactions

Convient aux environnements de génération de clés et de développement hors ligne, tout en assurant une prise en charge complète des algorithmes et des API. Idéal pour les déploiements BYOK (Bring Your Own Key) nécessitant la génération de clés de chiffrement avec une protection de niveau FIPS 140-2 avant de les exporter de manière sécurisée vers le cloud.

Grande portabilité

Sa petite taille, sa légèreté et son interface USB pratique permettent de prendre en charge de nombreuses plateformes, dont notamment les ordinateurs portables et autres appareils portables.

Rentable et évolutif

Le HSM Edge USB est le plus abordable de la gamme nShield. Il s'agit d'un HSM d'entrée de gamme qui vous permet de faire évoluer votre environnement en fonction de vos besoins. L'architecture Security World unique de Entrust vous permet d'associer plusieurs HSM nShield pour constituer un parc hybride évolutif qui vous permettra de partager des clés, d'équilibrer les charges et de bénéficier d'un basculement transparent.



Les HSM nShield Edge

INDICATIONS TECHNIQUES

Algorithmes de chiffrement supportés (dont la NIST Suite B intégrale)	Systèmes d'exploitation	Interfaces de Programmation d'Applications (APIs)	Compatibilité et évolutivité	Conformité en matière de sécurité
<ul style="list-style-type: none">Algorithmes asymétriques : RSA, Diffie-Hellman, ECMQV, DSA, El-Gamal, KCDSA, ECDSA, ECDH, Edwards (X25519, Ed25519ph)Algorithmes symétriques : 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, 3DESHachage / synthèse de message : MD5, SHA-1, SHA-2 (224, 256, 384, 512 bits), HAS-160, RIPEMD160	<ul style="list-style-type: none">Microsoft Windows 7 x64, 10 x64, Windows Server, 2012 R2 x64, 2016 x64, 2019 x64Red Hat Enterprise Linux AS/ES 6 x64, x86 and 7 x64 ; SUSE Enterprise Linux 11 x64 SP2, 12 x64, 15.1 x64Oracle Enterprise Linux 6.10 x64, 7.6 x64	<ul style="list-style-type: none">PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI et CNG, nCore, et Services Web (nécessite le pack d'options de services web)	<ul style="list-style-type: none">Port USB (conforme 1.x, 2.x)	<ul style="list-style-type: none">Norme FIPS 140-2, niveaux 2 et 3

Conformité aux normes de sécurité et d'environnement	Gestion et suivi	Caractéristiques matérielles	Performance
<ul style="list-style-type: none">UL, CE, FCC, RCM, et Canada ICES RoHS2, WEEE	<ul style="list-style-type: none">Enregistrement sécurisé des audits	<ul style="list-style-type: none">Appareil de bureau portable avec lecteur de carte à puce intégréDimensions lorsque le support est ouvert 120 x 118 x 27 mm (4,7 x 4,6 x 1 ")Poids : 340 g (0,8 lb)Tension d'entrée : 5 V DC alimenté par le dispositif hôte USBConsommation d'énergie : 700 mW	<ul style="list-style-type: none">Performance de signature pour les longueurs de clé recommandées NIST :2048 bits RSA : 2 tps4096 bits RSA : 0,2 tps

MODÈLES DISPONIBLES ET PERFORMANCE

- nShield Edge est proposé sous forme de modèles certifiés FIPS 140-2 de niveaux 2 et 3.
- Une version développeur non certifiée FIPS est également disponible

En savoir plus

Pour en savoir plus sur les HSM nShield de Entrust, rendez-vous sur entrust.com/fr/hsm. Pour en savoir plus sur les solutions de protection numérique de Entrust pour les identités, l'accès, les communications et les données, rendez-vous sur entrust.com/fr

Découvrez-en plus sur entrust.com/HSM

