



ENTRUST

Les HSM nShield Connect

La sécurité de vos applications dépend de l'endroit où vous conservez vos clés

CARACTÉRISTIQUES

Des fonctionnalités complètes

Les HSM nShield Connect sont des appareils certifiés FIPS 140-2 et Critères Communs EAL4+ (EN 419 221-5) qui fournissent des services de clés de chiffrement évolutifs et hautement disponibles sur les réseaux.

- Volumes de traitement d'opérations de chiffrement élevés et évolutivité à la demande
- S'intègrent à plus de 150 solutions de fournisseurs d'applications de premier plan
- CodeSafe constitue un environnement sécurisé pour l'exécution d'applications sensibles au sein d'appareils nShield.

Les HSM nShield Connect sont des appareils inviolables qui permettent de réaliser des fonctions telles que le chiffrement, la signature numérique, la génération et la protection de clés sur un grand nombre d'applications telles que :

- Les autorités de Certification
- La signature de code
- Les logiciels personnalisés
- Les applications cloud et conteneurisées
- Les service web
- La blockchain
- Le chiffrement de bases de données

La gamme nShield Connect comprend nShield Connect et le nouveau et ultra-performant nShield Connect XC.



DÉCOUVREZ-EN PLUS SUR [ENTRUST.COM/FR/HSM](https://www.entrust.com/fr/hsm)



Les HSM nShield Connect

PRINCIPAUX AVANTAGES ET FONCTIONNALITÉS

Architecture extrêmement flexible

Notre architecture Security World unique vous permet d'associer plusieurs HSM nShield pour constituer un parc hybride évolutif qui vous permettra d'équilibrer les charges et de bénéficier d'un basculement transparent.

Davantage de données traitées, et plus rapidement

Les HSM nShield Connect peuvent traiter de gros volumes chiffrés, ce qui les rend idéals pour les entreprises, les commerces de détails, l'IoT et d'autres environnements où le rendement est essentiel.

DE PUISSANTES FONCTIONNALITÉS À DISTANCE

Évitez de se rendre au centre de données

Administration nShield à distance - Cette fonctionnalité permet de présenter de manière sécurisée des cartes à puce d'autorisation à des HSM distants en vue d'exécuter des tâches de maintenance, telles que la mise à niveau des micrologiciels, la mise en service de nouveaux HSM et la réaffectation/reconfiguration des HSM existants. Fiche technique disponible.

Configuration à distance - La version console série de Connect XC permet une installation simple pour le personnel du centre de données, la configuration du réseau à distance et les réglages du panneau avant.

nShield Monitor fournit un tableau de bord unique regroupant tous vos HSM nShield pour vous aider à optimiser les opérations et à prolonger la durée de fonctionnement. Fiche technique disponible.

Protégez vos applications propriétaires

CodeSafe constitue un environnement sécurisé pour l'exécution d'applications sensibles au sein d'appareils nShield certifiés FIPS 140-2. Consultez la fiche technique de CodeSafe pour plus d'informations.

MODÈLES DISPONIBLES ET PERFORMANCE

Modèles nShield Connect	500+	XC Base	1500+	6000+	XC Mid	XC High
Performance de signature RSA (tps) pour les longueurs de clé recommandées NIST						
2 048 bits	150	430	450	3 000	3 500	8 600
4 096 bits	80	100	190	500	850	2 025
Performance de signature de courbe première ECC (tps) pour les longueurs de clé recommandées par le NIST						
256 bits	540	680	1 260	2 400	7 515 ²	14 400 ²
Licences client						
Incluses	3	3	3	3	3	3
Maximum	10	10	20	illimité ¹	20	illimité ¹

Annotation 1 : nécessite une licence client d'entreprise.

Annotation 2 : Les performances indiquées nécessitent l'activation de la fonction RNG rapide de ECDSA, disponible gratuitement sur demande auprès des équipes d'assistance de Entrust.



Les HSM nShield Connect

INDICATIONS TECHNIQUES

Algorithmes de chiffrement pris en charge (dont la NIST Suite B intégrale)	Plateformes prises en charge	Interfaces de Programmation d'Applications (APIs)	Connectivité des hôtes	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, 3DES Hachage / synthèse de message : MD5, SHA-1, SHA-2 (224, 256, 384, 512 bits), HAS-160, RIPEMD160 	<ul style="list-style-type: none"> Systèmes d'exploitation Windows et Linux, dont les distributions de RedHat, SUSE et des principaux fournisseurs de services cloud exécutés sous forme de machines virtuelles ou dans des conteneurs 	<ul style="list-style-type: none"> PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI/CNG et Services Web (nécessite le pack d'options de services web) 	<ul style="list-style-type: none"> Double port Gigabit Ethernet (deux segments de réseau) 	<ul style="list-style-type: none"> Certifié FIPS 140-2 niveau 2 et niveau 3 Certifié IPv6 et conforme à l'USGv6 Ready Connect XC : Certification eIDAS et Critères communs EAL4 + AVA_VAN.5 et ALC_FLR.2 conformément à la norme EN 419 221-5 relative au profil de protection, dans le cadre du régime néerlandais NSCIB Connect+ : Certifié Critères communs EAL4+ (AVA_VAN.5) Connect+ : Reconnu comme un dispositif de création de signature qualifiée Connect XC : Certifié BSI AIS 20/31

Conformité aux normes en matière de sécurité et d'environnement	Grande disponibilité	Gestion et suivi	Caractéristiques matérielles
<ul style="list-style-type: none"> UL, CE, FCC, RCM, Canada ICES RoHS2, WEEE 	<ul style="list-style-type: none"> Tous les SSD Ventilateur de service sur site, double alimentation à chaud 	<ul style="list-style-type: none"> Configuration nShield à distance (disponible sur les modèles Connect XC configurés par console série) Administration nShield à distance (à acheter séparément) nShield Monitor (à acheter séparément) Enregistrement sécurisé des audits Prise en charge des diagnostics Syslog et suivi des performances de Windows Agent de suivi SNMP 	<ul style="list-style-type: none"> Dimensions standard d'un rack 1U de 19" : 43,4 x 430 x 705 mm (1,7 x 16,9 x 27,8") Poids : 11,5 kg (25,4 lb) Tension d'entrée : 100-240 V CA à commutation automatique 50-60 Hz Consommation électrique : jusqu'à 2,0 A pour 110 V CA, 60 Hz 1,0 A pour 220 V CA, 50 Hz Dissipation de la chaleur : 327,6 à 362,0 BTU/h (pleine charge) Fiabilité - MTBF (heures)³, Connect XC : 107 384 heures, Connect+ : 99 284 heures

Annotation 3 : Calculé à une température d'exploitation de 25° C à l'aide de Telcordia SR-332 selon la norme MTBF « Reliability Prediction Procedure for Electronic Equipment ».

Pour en savoir plus
sur les HSM nShield
de Entrust

HSMinfo@entrust.com
entrust.com/fr/hsm

À PROPOS DE LA SOCIÉTÉ ENTRUST

Entrust sécurise un monde en mouvement avec des solutions qui protègent les identités, les paiements et les données, dans tous les pays. Aujourd'hui, les gens souhaitent des parcours plus fluides et plus sûrs quand ils traversent les frontières, font des achats, utilisent des services administratifs en ligne ou des réseaux d'entreprises. Notre portefeuille unique de solutions pour la sécurité numérique et l'émission de titres sécurisés permet de répondre précisément à ces souhaits. Grâce à nos 2500 collaborateurs, notre réseau international de partenaires et des clients dans plus de 150 pays, les organisations les plus fiables au monde nous font confiance.

Découvrez-en plus sur
entrust.com/HSM

