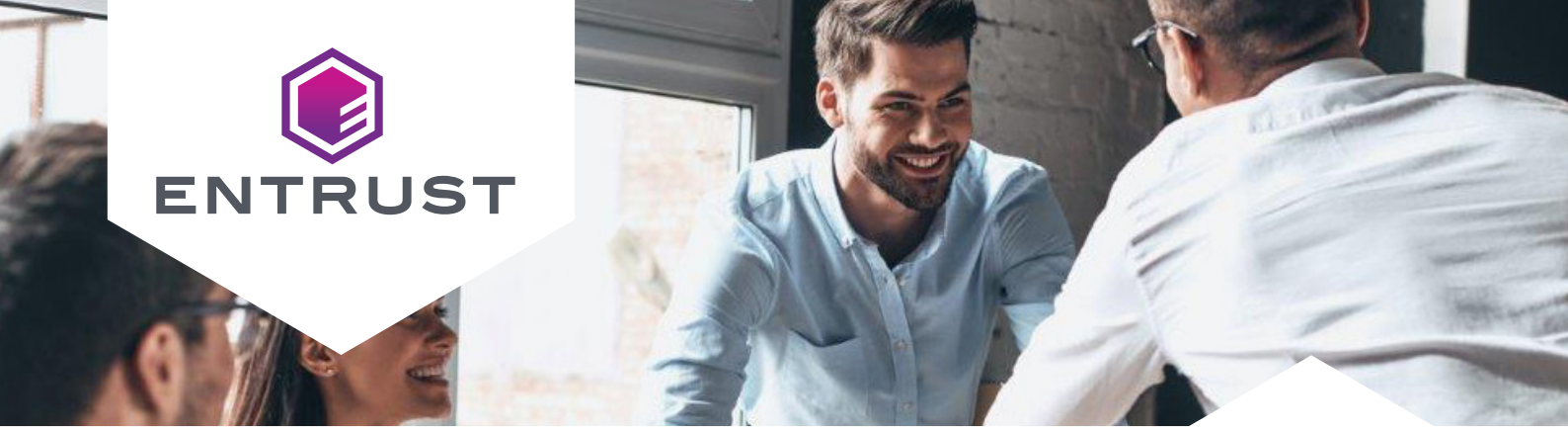


Les HSM nShield Solo

Cartes PCI-Express certifiées qui fournissent des services de clés de chiffrement aux serveurs autonomes

CARACTÉRISTIQUES

Les modules matériels de sécurité (HSM) nShield Solo sont des solutions certifiées FIPS sur carte PCI-Express de petite taille qui fournissent des services de chiffrement aux applications hébergées sur des serveurs ou des appareils. Ces cartes inviolables 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, notamment les autorités de certification, la signature de code, les logiciels personnalisés et bien d'autres encore.

La gamme nShield Solo comprend nShield Solo+ et le nouveau et ultra performant nShield Solo XC.

Architecture très évolutive

L'architecture Security World unique de Entrust 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

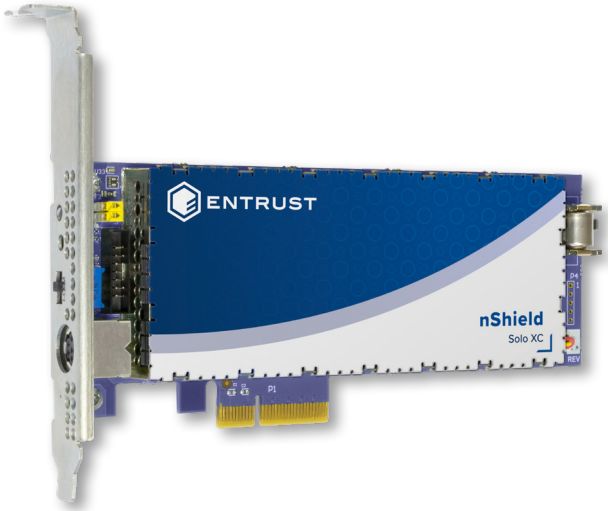
Les HSM nShield Solo peuvent traiter de gros volumes chiffrement, ce qui les rend idéals pour les entreprises, les commerces de détails, l'IoT et d'autres environnements où le rendement est essentiel.

Protégez vos données et applications propriétaires

CodeSafe constitue un environnement sécurisé pour l'exécution d'applications sensibles au sein d'appareils nShield.

PRINCIPAUX AVANTAGES ET FONCTIONNALITÉS

- Optimisation de la performance et de la disponibilité grâce à des volumes de traitement d'opérations de chiffrement élevés et à une évolutivité à la demande
- Prend en charge un large éventail d'applications, telles que les autorités de certification, la signature de code et plus encore
- nShield CodeSafe protège vos applications au sein de l'environnement d'exécution sécurisé de nShield
- L'administration à distance de nShield vous permet de limiter vos dépenses et vos déplacements



DÉCOUVREZ-EN PLUS SUR ENTRUST.COM/FR/HSM

Les HSM nShield Solo

INDICATIONS TECHNIQUES

Algorithmes de chiffrement pris en charge

- 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
- Mise en œuvre complète de la Suite B avec certification ECC complète, y compris Brainpool et courbes personnalisées

Plateformes prises en charge

- 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
- Environnements virtuels Solo XC pris en charge, notamment VMware ESX, Microsoft Hyper-V, Linux KVM et Citrix XenServer

Interfaces de Programmation d'Applications (APIs)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI et CNG, nCore, et Services Web (nécessite le pack d'options de services web)

Connectivité des hôtes

- PCI Express Version 2.0 ; connecteur Solo+ : 1 voie, connecteur Solo XC : 4 voies

Conformité en matière de sécurité

- Certifié FIPS 140-2 niveau 2 et niveau 3
- Solo+ : Certifié Critères communs EAL4+ (AVA_VAN.5)
- Solo+ reconnu comme un dispositif de création de signature qualifiée
- Solo 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
- Solo XC : Certifié BSI AIS 20/31

Conformité aux normes en matière de sécurité et d'environnement

- UL, UL/CA, CE, FCC, Canada ICES, KC, FCC, VCCI, RCM
- RoHS2, WEEE, REACH

Gestion et suivi

- Administration à distance nShield et nShield Monitor
- Enregistrement sécurisé des audits
- Prise en charge des diagnostics Syslog et suivi des performances de Windows
- Agent de suivi SNMP

MODÈLES DISPONIBLES ET PERFORMANCE

Modèle nShield Solo	500+	XC Base	6000+	XC Mid	XC High
Performance de signature RSA (tps) pour les longueurs de clé recommandées NIST					
2 048 bits	150	430	3 000	3 500	8 600
4 096 bits	80	100	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	2 400	7 515[1]	14 400[1]

Dimensions	Poids		Puissance	
	Solo+	Solo XC	Solo+	Solo XC
56,2 Q 167,1 Q 15,4 mm	230 g	280 g	10 W	24 W
2,2 Q 6,6 Q 0,6 in	0,5 lb	0,62 lb		

Annotation 1 : Les performances indiquées nécessitent l'activation de la fonction RNG rapide de ECDSA, disponible gratuitement sur demande auprès des équipes d'assistance de Entrust.

Découvrez-en plus sur
entrust.com/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com