

## nShield Connect

- Maximise les performances et la disponibilité grâce à des vitesses de transaction chiffrée élevées et une extensibilité flexible
- Prend en charge une large variété d'applications, y compris des autorités de certification, signature de code et autres
- nShield CodeSafe protège vos applications au sein de l'environnement d'exécution sécurisé de nShield
- nShield Remote Administration vous aide à réduire vos coûts et temps de trajets



## HSM nShield Connect

*Dispositifs certifiés offrant des services de clé de chiffrement sur les réseaux*



# HSM nShield Connect

## Présentation des fonctionnalités



Les HSM nShield Connect sont des dispositifs certifiés FIPS délivrant des services de clé de chiffrement aux applications sur toute l'étendue de votre réseau. Ces plateformes à sécurité renforcée exécutent notamment des fonctions de chiffrement, de signature numérique, ou encore de protection et de génération de clés sur un large éventail d'applications, y compris pour les autorités de certification, la signature de code, la personnalisation de logiciels et plus encore.

La gamme nShield Connect comprend le modèle nShield Connect+ et le nouveau modèle hautes performances nShield Connect XC.

### ARCHITECTURE HAUTE FLEXIBILITÉ

L'architecture unique Security World de nCipher permet de combiner les différents modèles de HSM nShield afin de composer un parc mixte offrant flexibilité d'expansion et fluidité de basculement et d'équilibrage des charges.

### TRAITEMENT DE DONNÉES ACCÉLÉRÉ

Prenant en charge des vitesses de transaction élevées, les HSM nShield Connect s'avèrent particulièrement adaptés aux environnements d'entreprise, de commerce de détail, d'IoT et autres, dans lesquels le débit est un facteur critique.

### PROTÉGEZ VOS APPLICATIONS PROPRIÉTAIRES

L'option CodeSafe fournit un environnement sécurisé pour l'exécution d'applications sensibles au sein de nShield.

### CARACTÉRISTIQUES 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, Triple DES
- Hachage: MD5, SHA-1, SHA-2 (224, 256, 384, 512 bits), HAS-160, RIPEMD160
- Implémentation de l'ensemble de la Suite B avec licence intégrale pour l'utilisation d'ECC, y compris Brainpool et courbes personnalisées

#### Systèmes d'exploitation pris en charge

- Microsoft Windows 7 x64, 10 x64 ; Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- Red Hat Enterprise Linux AS/ES 6 x64, 6 x86, 7 x64; 5 x64 (libc6.5) (prise en charge partielle), SUSE Enterprise Linux 11 x64 SP2, 12 x64
- Oracle Solaris 11 (SPARC), Oracle Solaris 11 x64
- IBM AIX 7.1 (POWER6, POWER8), HP-UX 11i v3
- Oracle Enterprise Linux 6.8 x64 et 7.1 x64

#### Interfaces de programmation d'applications (API)

- PKCS#11, OpenSSL, Java (JCE), Microsoft CAPI et CNG, nCore, nShield Web Services Crypto API

#### Connectivité hôte

- Deux ports Gigabit Ethernet (deux segments de réseau)

#### Conformité aux exigences de sécurité

- Certification FIPS 140-2 niveau 2 et niveau 3

- Certification IPv6 et conformité USGv6 Ready
- Connect+: Certification Critères Communs EAL4+ (AVA\_VAN.5)
- Connect+ reconnu en tant que dispositif de création de signature qualifié
- Connect XC: Conformité BSI AIS 20/31

#### Conformité aux normes environnementales et de sûreté

- UL, CE, FCC, C-TICK, Canada ICES RoHS2, DEEE

#### Haute disponibilité

- Stockage intégral sur disque dur SSD
- Composants réparables sur site, double alimentation à basculement sans interruption

#### Gestion et surveillance

- nShield Remote Administration et nShield Monitor
- Consignation d'audit sécurisée
- Prise en charge des diagnostics syslog et suivi de performances de Windows
- Agent de surveillance SNMP

#### Caractéristiques physiques

- Rack standard 1U 19 pouces Dimensions: 43,4 x 430 x 705 mm (1,7 x 16,9 x 27,8 in)
- Poids: 11,5 kg (25,4 lb)
- Tension d'entrée: 100-240 V CA basculement automatique 50-60Hz
- Consommation électrique : jusqu'à 2,0 A à 110 V CA, 60 Hz | 1,0 A à 220 V CA, 50 Hz
- Dissipation thermique: 327,6 à 362,0 BTU/h (pleine charge)

### MODÈLES DISPONIBLES ET PERFORMANCES

Modèles nShield Connect	500+	XC Base	1500+	6000+	XC Mid	XC High
Performances de signature RSA (tps) pour NIST Longueur de clé recommandée						
2048 bits	150	430	450	3,000	3,500	8,600
4096 bits	80	100	190	500	850	2,025
Performances de signature pour courbes ECC sur corps fini (tps) pour NIST Longueur de clé recommandée						
256 bits	540	680	1,260	2,400	5,500	14,400
Licences client						
Incluses	3	3	3	3	3	3
Maximum	10	10	20	100	20	100

### EN SAVOIR PLUS

Pour découvrir comment nCipher Security incorpore confiance, intégrité et contrôle aux informations et applications critiques de votre entreprise, accédez à [ncipher.com](http://ncipher.com)

Search: [ncipher.com](http://ncipher.com)



©nCipher - November 2019 - PLB 889C

[www.ncipher.com](http://www.ncipher.com)

