nCIPHER
AN ENTRUST DATACARD COMPANY

www.ncipher.com

nShield Connect

- 具備高速加密交易和靈活擴展性能，實現效能和可用性的最大化
- 支援廣泛的應用系統，包括憑證授權、程式碼簽章（code signing）及更多
- nShield CodeSafe可在 nShield 的安全執行環境中保護您的應用系統及商業邏輯
- nShield 遠端管理（Remote Administration）、配置（ Remote Configuration）及監控系統（Monitor）的選項助您減少交通需求並更有效管理HSMs

nShield Connect 硬體安全模組（HSMs）

經認證可提供具靈活擴展性及高度可用性之跨網絡加密金鑰服務的設備

nShield Connect
硬體安全模組 (HSMs)
功能概述

nShield Connect HSMs 是符合美國聯邦資訊處理標準（FIPS）140-2及通用標準 EAL4+（EN 419 221-5）認證的設備，可為網路上的應用系統提供加密服務。這些防篡改的平台可以在廣泛的應用系統中執行加密、數位簽章及金鑰生成與保護等功能，當中包括憑證機構（ca）、程式碼簽章、自行開發軟體及更多。

nShield Connect 系列包括 nShield Connect+和高效能 nShield Connect XC。

高度靈活架構

nCipher 獨特的Security World架構可讓您結合不同的nShield HSM系列產品來建立一個混合架構，實現靈活擴展以及無縫故障轉移和負載平衡。

更快地處理更多數據

nShield Connect HSMs 支援高交易頻率，是企業、零售業、物聯網及其他着重高吞吐量之應用環境的理想選擇。

保護您的專屬應用系統

CodeSafe方案為您提供一個安全的環境，在 nShield 防護範圍內運行機密應用系統。

技術規格

支援的加密演算法

- 非對稱演算法：RSA、Diffie-Hellman、ECMQV、DSA、ElGamal、KCDSA、ECDSA（包括NIST、Brainpool及secp256k1曲線）、ECDH、Edwards（Ed25519、Ed25519ph）、X25519
- 對稱演算法：AES、Arcfour、ARIA、Camellia、CAST、MD5 HMAC、RIPEMD160 HMAC、SEED、SHA-1 HMAC、SHA-224 HMAC、SHA-256 HMAC、SHA-384 HMAC、SHA-512 HMAC、Tiger HMAC、Triple DES
- 雜湊/訊息摘要演算法：MD5、SHA-1、SHA-2（224、256、384、512 位元）、HAS-160、RIPEMD160
- 獲得NIST Suite B認證的演算法

支援的作業系統

- Microsoft Windows 7 x64、10 x64；Windows Server、2012 R2 x64、2016 x64、2019 Core x64、2019 x64
- Red Hat Enterprise Linux AS/ES 6 x64、6 x86、7 x64；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 與7.1 x64

應用程式介面（APIs）

- PKCS#11、OpenSSL、Java（JCE）、Microsoft CAPI和CNG、nCore、及與Web Services Option Pack結合使用的nShield Web Services API

主機連線

- Gigabit乙太網路雙連接埠（兩個網路區段）

安全合規

- FIPS 140-2第2 級和第3 級認證
- IPv6認證並符合USGv6標準
- Connect XC：針對荷蘭認證機構NSCIB第EN 419 221-5號保護總則之elDAS及通用標準 EAL4+ AVA_VAN.5和ALC_FLR.2認證
- Connect+：通用標準 EAL4+（AVA_VAN.5）認證
- Connect+：認可為簽名生成合規設備
- Connect XC：符合BSI AIS 20/31標準

符合安全和環境標準

- UL、CE、FCC、RCM、加拿大 ICES RoHS2、WEEE

高可用性

- 全為固態儲存設備
- 可現場置換的風扇架，雙熱插拔電源供應器

管理及監控

- nShield 遠端配置（Remote Configuration）(可用於已配置序列主控台的Connect XC型號)
- nShield 遠端管理（Remote Administration）（需另外購買）
- nShield監控系統（Monitor）（需另外購買）
- 安全稽核記錄
- Syslog 診斷支援與 Windows 效能監控
- SNMP監控代理

外型特徵

- 標準 1U 19 英吋 機架安裝尺寸：43.4 x 430 x 705 公釐 (1.7 x 16.9 x 27.8 英吋)
- 重量：11.5公斤（25.4磅）
- 輸入電壓：AC 100-240V，50/60Hz，自動切換
- 功耗：AC 110V時最高可達2.0A，60Hz | AC 220V 時為 1.0A ，50Hz
- 可靠度：平均故障間隔 (MTBF)（小時）[1]
  - Connect XC: 107,384小時
  - Connect+: 99,284小時
- 散熱：每小時327.6至362.0英熱单位（滿負荷）

注1：於25°C的運轉溫度下，使用Telcordia SR-332「Reliability Prediction Procedure for Electronic Equipment」平均故障間隔散熱標準計算：327.6至362.0 BTU /小時（滿載）

可選型號與效能

nShield Connect 型號	500+	XC 基本	1500+	6000+	XC 中級	XC 高級
適用於NIST的RSA 運算效能 (tps) 建議金鑰長度						
2048 位元	150	430	450	3,000	3,500	8,600
4096 位元	80	100	190	500	850	2,025
適用於NIST的ECC Prime Curve 運算效能 (tps) 建議金鑰長度						
256 位元	540	1,210	1,260	2,400	7,515	14,400
用戶端授權						
包含	3	3	3	3	3	3
最多	10	10	20	無限制*	20	無限制*

了解更多

若要進一步了解 nCipher Security 如何為您關鍵的資料與應用系統提供可信度，確保資料的完整性，並給予您充分的管控力，請造訪 nCipher.com。