

全球第一品牌的硬體安全模組(HSM)

當企業或組織在建置加解密硬體來保護它們的資訊安全基礎建設時，必須考量其靈活性與彈性。netHSM是一台高效能、可被分享的網路型硬體加密器(HSM)，讓您的企業或組織在未來有擴充需求時，將netHSM用於新的需求上

可分享的安全資源

HSM是一種提供加解密服務的硬體平台以加強多種應用程式的安全—從PKI、系統認證、網路服務到SSL加密連線。nCIPHER的netHSM就像一台網路型的安全加解密處理機，可以讓多台的伺服器安全地連線到單一台的netHSM上並要求netHSM提供與之相應的加解密功能，就如同每一台伺服器都配有一台專屬的HSM一樣，而您在HSM設備上的全部花費卻比每台伺服器都配一台專屬的HSM要少得多，而系統的管理卻因之簡化易行。



建立一個高效能的加解密平台

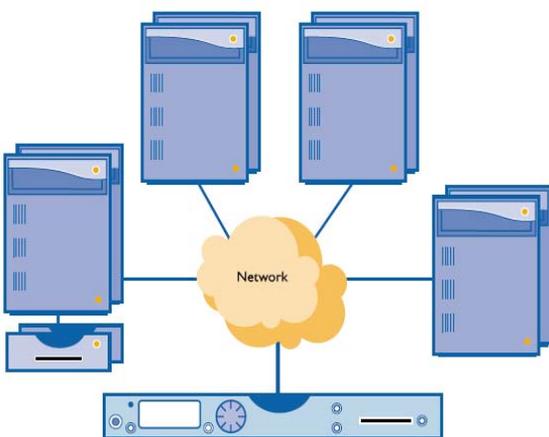
nCIPHER的Security World提供最好的金鑰管理模式及存取控管，安全應用程式可以受到netHSM的保護。netHSM並不限制其可保護的金鑰數量，並支援多達20台的伺服器可同時連接使用。

唯有通過FIPS Level 3認證的硬體加密器才能確保金鑰的安全無虞。nCIPHER的netHSM在安全的設計上提供以下的防護：

- FIPS 140-2 Level 3認證的保護來保護金鑰
- 加密的網路連線傳輸
- 強化的伺服器登入、連線認證
- 在網路上隱形以防止來自網路的攻擊
- 強化的工作機制，確保內部系統軟體的正確性
- 安全及整合式的使用者介面

nCIPHER的toolkits能讓客製化的安全應用程式充分使用由netHSM所提供的好處，如金鑰管理、硬體保護及高速加解密運算處理。

Flexible deployment



Allows multiple servers to securely access a single HSM

netHSM 特點	使用益處
可共享的加解密資源	提供彈性的安全予多台伺服器及站台，因而降低在HSM上的花費
通過完整的FIPS 140-2認證	netHSM為硬體的鑰匙保護提供經FIPS 140-2 Level 3 等級認證地安全保護
高容量	netHSM可以保護無限大數目的鑰匙，可供多達20台的伺服器來做加解密運算
完全相容現存的nCipher HSM部署	可以將以前的設定保留上來
安全的使用者介面	整合式地安全使用者介面不需要透過其他的設備或伺服器來啟動
鑰匙分持	鑰匙可以分持至幾個授權的人員，以防止非法的使用(K of N)
高效性能：2000 TPS	每秒可處理2000個1024 bit的鑰匙加解密運算
備援及負載平衡	netHSM可以被佈署至HA系統中，並與其他HSM結合在同一安全系統內以達到備援及負載平衡
完整的API及廣泛的AP支援	透過nCipher既有的API，與AP的整合變得非常簡單

技術規格

應用程式介面(APIs)

- ✓ PKCS#11
- ✓ CSP for Microsoft CryptoAPI
- ✓ Java JCA/JCE CSP
- ✓ OpenSSL
- ✓ BHAPI
- ✓ 'nCore' API 'C' or Java
- ✓ CHIL

對稱式加密演算法

- ✓ Triple-DES (two and three key)
- ✓ AES - Rijndael
- ✓ Arc Four (compatible with RC4)
- ✓ CAST
- ✓ DES

執行效能

- ✓ 非對稱運算: 2000TPS (RSA1024 bit)

公開鑰匙加密演算法

- ✓ DSA
- ✓ ECDSA
- ✓ El Gamal
- ✓ RSA

Key exchange mechanisms

- ✓ DH
- ✓ EC-DH (optional on netHSM 800 only)
- ✓ DES / DES3 XOR

雜湊函數 and 雜湊訊息身份驗證代碼(HMAC)

- ✓ MD2, MD5
- ✓ RIPEMD 160
- ✓ SHA-2, SHA-1
- ✓ DES-MAC
- ✓ 3DES-MAC

