netHSM™

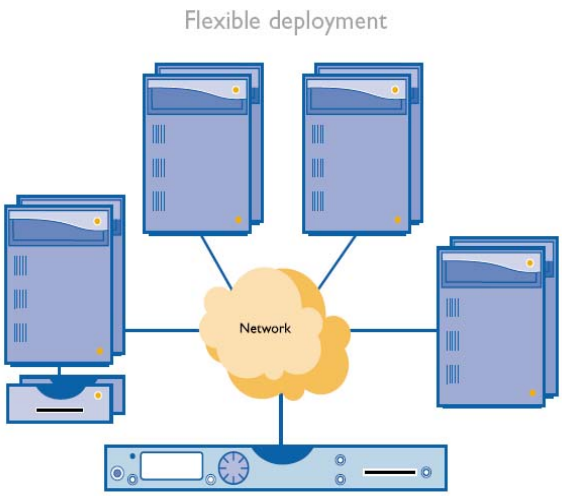
NETWORK-CONNECTED HARDWARE SECURITY MODULE (HSM)

重新定義加解密硬體的投資報酬率

當企業或組織在使用加解密硬體來保護它們的資訊基礎建設時，該加解密硬體是否有佈置的靈活性與彈性是非常地重要！netHSM是一台能分享的網路型硬體加密器(HSM)，能讓您的企業或組織在未來有需求時，將netHSM用於新的需求上，不用另外再買一台硬體加密器(HSM)；而且，netHSM完全相容於nCipher其他類型的HSM。

nCipher的netHSM是一個可提供加解密服務的平台，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。

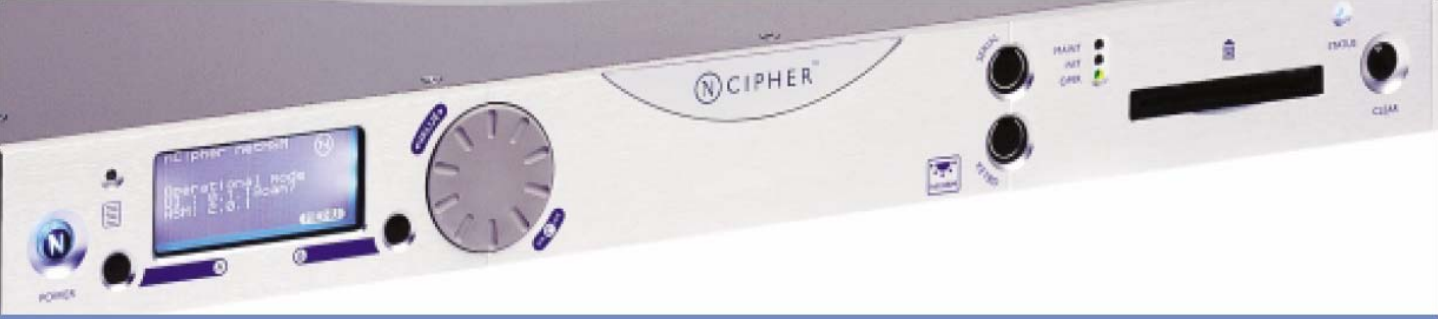
netHSM就像一台網路型的安全加解密處理機，相較於傳統式的一台HSM配一台伺服器，netHSM是另一種更佳的選擇。您可以讓多台的伺服器安全地連線到單一台的netHSM上並要求netHSM提供與之相應的加解密功能，就如同每一台伺服器都配有一台專屬的HSM一樣，而您在HSM設備上的全部花費卻比每台伺服器都配一台專屬的HSM要少得多，而系統的管理卻因之簡化易行。



Allows multiple servers to securely access a single HSM

- ■可共享的HSM
- ■FIPS 140-2 Level 3 安全等級認證
- ■多層的安全架構
- ■安全的網路連線
- ■安全的使用者介面
- ■強力的需求服務認證機制
- ■運算效能達 2000 TPS
- ■標準1U網路設備大小
- ■支援ECC演算法

nCIPHER™



NETWORK CONNECTED HARDWARE SECURITY MODULE (HSM)

安全上的設計

- FIPS 140-2 Level 3安全等級保護金鑰
- 加密的網路連線傳輸
- 強力的伺服器登入、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，以確保內部系統軟體的正確性
- 安全及整合式的使用者介面

易共用與靈活性

所有的nCipher硬體加密器都是使用相同的金鑰管理架構－nCipher's Security World。因爲如此，netHSM可以完全地與nCipher「專屬型硬體加密器」整合與共用。所以，nCipher的硬體加密器可以按照組織的需求來作任何形式的調配佈置。

管理性

傳統上，當網路擴充時，與之相應的安全機制亦隨之擴充。若是使用專屬型的HSM，則在網路擴充時所需耗費的時間與人力亦大大地增加，特別是，當網路的架構橫跨兩地、三地或更多地時，在分散各地的HSM上的建置與管理成本將大幅上昇。唯有集中式管理HSM，才能降低管理成本，透過netHSM，各地的伺服器經由安全的網路連線及認證而連至netHSM並享有相同的FIPS等級的加解密作業。

整合的一致性

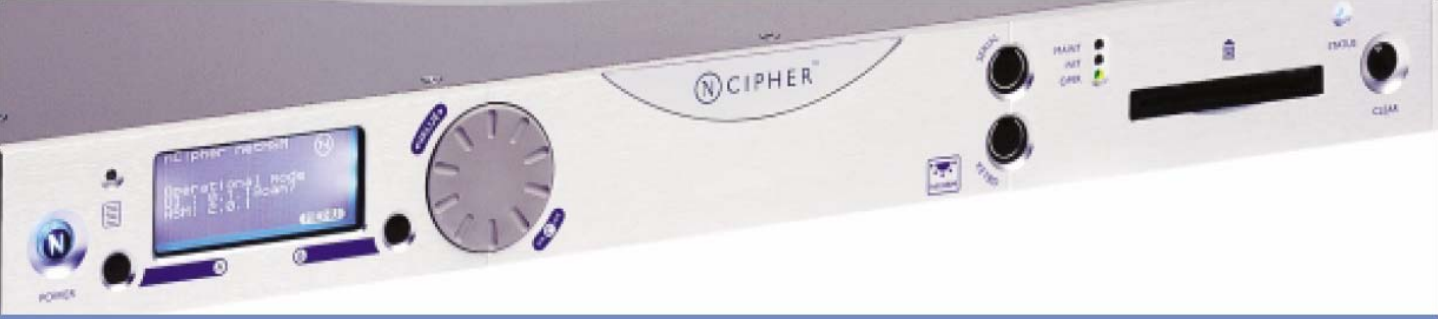
多年來，nCipher的客戶在客製化或商業化的安全應用上已經使用我們的toolkits來和我們的「專屬型硬體加密器」做整合。因爲netHSM是完全相容於所有的nCipher「專屬型硬體加密器」，同樣的toolkits可用來整合netHSM，由此，可以快速及有效地將netHSM整合至現有的安全應用中。

高效性能

由於有netHSM來作有關加解密的作業，凡是連到netHSM的伺服器，都不需將系統的資源花在加解密運算上，因此，系統的整體效能得到提昇。netHSM的非對稱式運算效能高達每秒2000次(TPS)

再者，netHSM的大小是1U高，19吋寬，僅佔一個rack機器的槽。

nCIPHER™



NETWORK CONNECTED HARDWARE SECURITY MODULE (HSM)

可昇級的加解密平台

nCipher的Security World提供最好的金鑰管理模式及存取控管，並且避免了安全上孤兒程式的產生，只要有需要，安全應用程式就可以受到netHSM的保護。netHSM並不限制其可保護的金鑰數量，並支援至20台的伺服器。

建立一個企業級的加解密政策

許多企業組織開始在單一伺服器上使用硬體保護加密器，例如，含有SSL的網頁伺服器。對這個應用來說，一台「專屬型硬體加密器」就夠了。然而，當愈來愈多在加解密上的應用需求隨著企業組織的成長而增加時，爲每一台有加解密需求的伺服器配一台「專屬型硬體加密器」就不符合經濟效益。這時一台netHSM不僅可以供多台的伺服器使用，還可供分處兩地以上的伺服器使用，更可與之前買的「專屬型硬體加密器」整合。

netHSM 的開發工具

nCipher的toolkits提供業界標準的API, 能讓客製化的安全應用程式儘量使用由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。SEE (應用程式碼載入HSM內執行)的功能使得應用系統更安全

硬體保護遠端伺服器的登入認證

爲了更加加強系統的安全，netHSM對於遠端伺服器的登入認證上，更提供了硬體的token 給連線至netHSM的伺服器，以加強netHSM與伺服器間的認證。這個機制，不但

金鑰安全與管理

密碼金鑰是整個加解密作業中最重要的部份。在保護及管理這些密碼金鑰上的一點錯誤，其影響是廣及整個安全層級。許多的企業組織都犯了一個很大的錯誤，那就是將這些密碼金鑰用所謂的「軟體安全」來保護，意即用另一把加密金鑰透過某一演算法來對要被保護的密碼金鑰做加密，而這把金鑰則留在伺服器上。殊不知，這把未受任何保護的金鑰將是整個安全上最大的漏洞。

但凡有敏感的資料需用到加密技術來保護，企業組織都應佈署「硬體安全」來做風險控管，而「硬體安全」最重要的就是由「硬體加密器」來保護金鑰。netHSM是通過FIPS 140-2 Leve 3的認證，所以，凡是受到netHSM保護的金鑰，都是受到FIPS 140-2 Leve 3的保護。

除了FIPS上的認證外，nCipher也延請了公證的第三方來測試netHSM在網路上的安全，而驗證了netHSM可防止來自網路層面的攻擊。

nCIPHER™

netHSM™ NETWORK CONNECTED HARDWARE SECURITY MODULE (HSM)

技術規格

連接介面
- 2 * 10/ 100 Ethernet
- RS232, mini DIN serial connection
- PS/2 keyboard connection

使用者介面
- High Resolution Graphic LCD
- Two ‘Soft’ menu keys
- Scroll / select knob
- IC Card Reader

作業系統
- AIX, HP-UX, Solaris
- Linux
- Windows

體積大小
- Weight 6.4 Kg
- Standard 1U rack mount

電源
- Input voltage 100-240 AC auto switching 50-60±10Hz (nominal)
- Maximum Power Consumption: 460 watts (4 amps at 115 volts AC)

溫度濕度
- +10 to +35 degC; 10 to 85% relative humidity, non condensing

認證
- FCC: CFR47, Part 15, Subpart B, Class A
- CE: EN55022, Class A; EN55024-1; EN60950
- FIPS 140-2 Level 3
- RoHS Compliant

效能 (1024 bit RSA key)
- netHSM 500:500 TPS
- netHSM 2000:2000 TPS

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

支援演算法
- SYMMETRIC CIPHERS
  AES – Rijndael
  Arc Four (compatible with RC4)
  CAST
  DES
  Triple-DES
- PUBLIC KEY CIPHERS
  DSA
  El Gamal
  RSA (up 4096 bits)
- KEY EXCHANGE
  DH
  DES / DES3 XOR
- HASH AND HMAC
  MD2
  MD5
  RIPEMD 160
  SHA-2
  SHA-1

其它
- Remote Operator
- SEE (Secure Execution Engine)
- ISO Smartcard Support
- Elliptic Curve ['ECC'] Activation

**http://www.ncipher.com/cryptographic_hardware/hardware_security_modules/10/nethsm

nCIPHER™