netHSM™

NETWORK-CONNECTED HARDWARE SECURITY MODULE (HSM)

重新定義加解密硬體的投資報酬率

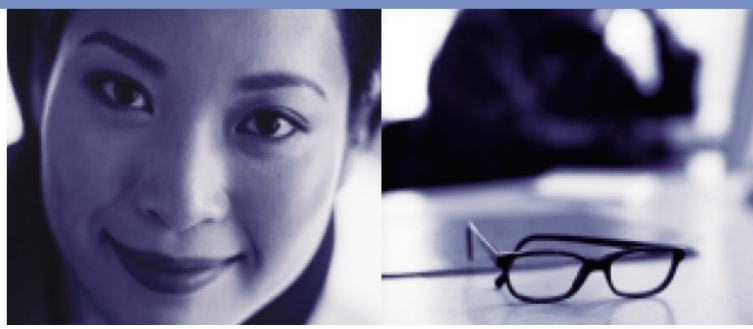
當企業或組織在使用加解密硬體來保護它們的資訊基礎建設時，該加解密硬體是否有佈置的靈活性與彈性是非常重要地！netHSM是一台能分享的網路型硬體加密器(HSM)，能讓您的企業或組織在未來有需求時，將netHSM用於新的需求上，不用另外再買一台硬體加密器(HSM)；而且，netHSM完全相容於nCipher其他類型的HSM。

可分享的安全資源

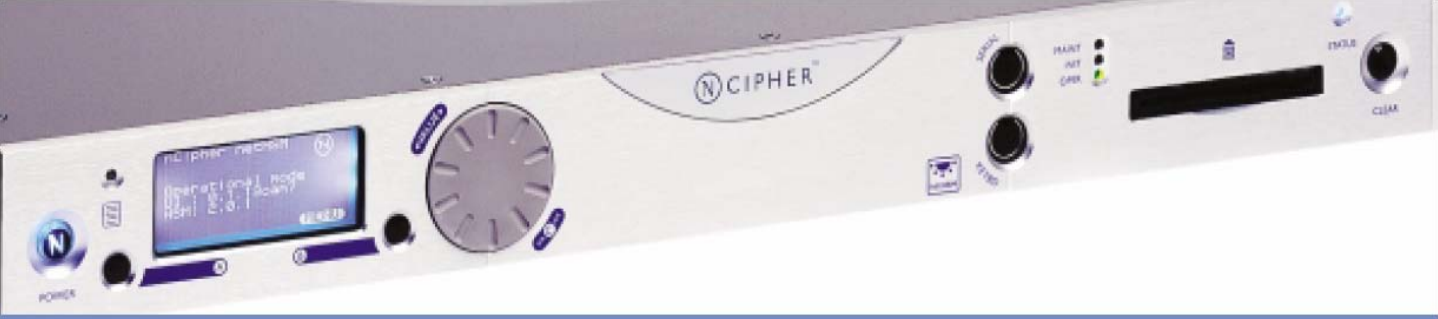
netHSM是一個可提供加解密服務的平台以加強多種應用程式的安全－從PKI、系統認證、網路服務到SSL加密連線。

nCipher的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。

netHSM™



FEATURE 特點	BENEFIT 益處
可享的加解密資源	提供彈性化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為硬體的金鑰保護提供經FIPS 140-2等級認證地安全保護
高容量	netHSM可以保護無限大數目的金鑰，並提供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
金鑰分持	金鑰可以分持至幾個授權的人員，以防止非法的使用
高效性能：1600TPS	每秒可處理1600個1024 bit的金鑰加解密運算
備援及負載平衡	netHSM可以被佈署至HA系統中，並與專屬型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

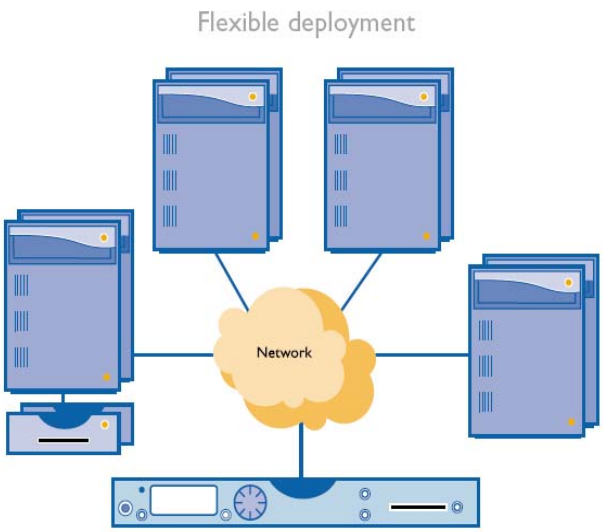


NETWORK CONNECTED HARDWARE SECURITY MODULE (HSM)

安全上的設計

因為加解密處理流程的安全與保護就如同個人的銀行密碼一樣重要，唯有通過**FIPS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
- 強化地伺服器登入、連線認證
- 在網路上隱形，以防止來自網路的攻擊
- 強化地工作機制，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



Allows multiple servers to securely access a single HSM

管理性

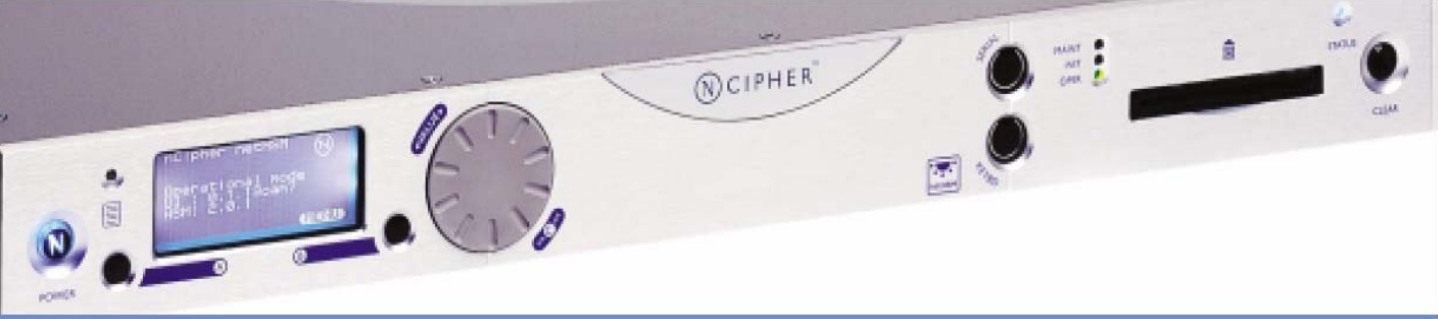
傳統上，當網路擴充時，與之相應的安全機制亦隨之擴充。若是使用專屬型的HSM，則在網路擴充時所需耗費的時間與人力亦大大地增加，特別是，當網路的架構橫跨兩地、三地或更多地時，在分散各地的HSM上的建置與管理成本將大幅上昇。唯有集中式管理HSM，才能降低管理成本，透過netHSM，各地的伺服器經由安全的網路連線及認證而連至netHSM並享有相同的FIPS等級的加解密作業。

在集中管理方面，nCipher除了提供Smartcard來做人員認證外，netHSM也允許透過遠端登入的方式來作一些管理的工作。遠端人員可以用Smartcard透過任一伺服器與一台專屬型HSM並經由安全的連線來與netHSM連線作業。

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。再者，netHSM的大小是1U高，19吋寬，僅佔一個rack機器的槽。

分享式的加解密硬體對需要用到複數的硬體或是機房分散於各地的組織與企業來說，可以省下硬體的費用、管理的費用及人員至各地維護的費用，換言之，就是增加ROI－投資報酬率。



NETWORK CONNECTED HARDWARE SECURITY MODULE (HSM)

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。因為如此，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。

配置上的靈活性使得企業組織得以保護現存的投資，當有需要時，經由重新的配置與硬體的重新規劃，企業組織的資安架構輕易地就可符合新的商業需求，這不啻是將資訊安全的投資最大化。

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。因為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。

快速的整合及配置，使企業組織能有效率地符合法規規範。

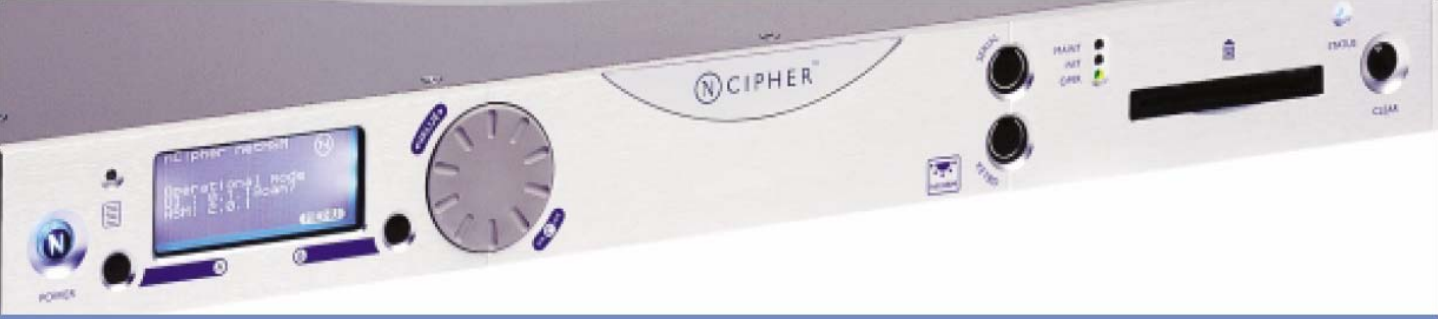
可昇級的加解密平台

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。

netHSM的設定是由商業需求及安全政策來決定，而非有所限制的科技技術。

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，為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。



NETWORK CONNECTED HARDWARE SECURITY MODULE (HSM)

獨立地安全驗證

密碼金鑰是整個加解密作業中最核心、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，最重要的是，netHSM整台機器通過認證，而不只是其中的一部份，所以，但凡受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因其可在網路上隱形，故可防止來自網路層面的攻擊。

硬體保護遠端伺服器的登入認證

為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，不但防止非法的金鑰使用，更加強了點對點之間的安全。

netHSM及客製化的安全

nCipher的toolkits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。

產品規格

產品	連接介面	FIPS 140-2 認證等級	每秒可處理之1024 bit SSL連線
netHSM 1600	10/100 Ethernet	Level 3	1600
netHSM 300	10/100 Ethernet	Level 3	300
netHSM 800	10/100 Ethernet	Level 3	800

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

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

演算法

對稱式加密演算法

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

公開金鑰加密演算法

- DSA
- ECDSA (optional on netHSM 800 only)
- 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

效能

netHSM 300
- 300 TPS (1024 bit RSA keys)
- 1MB TPS (3DES keys)

netHSM 800
- 800 TPS (1024 bit RSA keys)
- 4.45MB TPS (3DES keys)
- 4.23MB TPS (AES-256 keys)

netHSM 1600
- 1600 TPS (1024 bit RSA keys)
- 400 TPS (2048 bit RSA keys)
- 1MB TPS (3DES keys)

netHSM™ NETWORK CONNECTED HARDWARE SECURITY MODULE (HSM)

作業系統

- Windows 2000 SP4
  - Qualified by Microsoft *Designed for Microsoft Windows 2000* testing program
- Windows 2003 and 2003 SP1
- Solaris 7 (32 and 64 bit), Solaris 8, Solaris 9
  - Qualified by Sun *Solaris Ready* testing program
- Linux Libc 6.2, kernels 2.4.0 and up
  - Linux只要Libc及kernels有支援，不論何種安裝套件皆支援
- AIX 4.X and above, 5.1 (32 and 64 bit), AIX 5.2
- HPUX 11 (32 and 64 bit), HPUX 11i

Mechanical

- Weight 6.4 Kg
- Standard 1U rack mount [19" x 1.75 x 17.25], (482mm x 44mm x 440mm)

Electrical

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

Certification

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

Temperature / Humidity (Operational):
+10 to +35 degC; 10 to 85% relative humidity, non condensing