nCipher Key Management

(金鑰管理)

隨著對資訊安全的重視，用金鑰來加密敏感資料的應用愈來愈多，然而，在這方面資訊安全上的顧慮，也從敏感資料轉移到金鑰上來，爲了保護這些金鑰，HSM(Hardware Security Module)－「硬體加密器」也隨之因應而生。

但是，HSM 雖然保護住了這些金鑰，對於金鑰的產生、使用、管理、儲存及銷毀並不完全，而協助 HSM 達到對金鑰的產生、使用、管理、儲存及銷毀這些的流程，就是金鑰管理－Key Management

有些專有名詞需要先行釐清以畀容易了解本文。
Master Key = Root key = Module Key = Wrapper Key = 加密金鑰
HSM = Hardware Security Module = 硬體加解密模組 = 硬體加密器

金鑰管理的目的

對於金鑰管理的目的，主要有三大要點：

1. Security(安全性): 不是任何人都可使用金鑰，唯有被授權的使用者，在其被授權的場所內，方可使用金鑰！

2. Robustness(活力性): 但凡有所需時，金鑰就必須得發揮其功用，也就是隨傳隨到，即便是「系統故障」、「人員離職」或是「硬體損毀」，金鑰的功用亦不可因上述之原由而有被絲毫的影響。

3. Scalability(可擴充性): 企業組織對系統需求的增加與日俱增，金鑰的數目及對金鑰使用的需求也隨之遞增，所以，更多的金鑰管理方面的需求也隨之而來。如何在日益複雜的系統環境中，乃能保持對金鑰管理的需求，是非常的重要。

金鑰管理的兩難

在金鑰管理上，使用者常面臨到一個關鍵而兩難的決定是「到底是把所有的金鑰存放在硬體加密器裡好，還是把所有的金鑰用另一把金鑰(如 Master Key)加密後，只要把那把加密所有金鑰的金鑰存放在硬體加密器裡就可以了呢？」

傳統的說法是：「金鑰應該存放在硬體加密器裡」－ Stay in the box，然而，把所有的金鑰鎖在硬體加密器裡卻很大限度地犧牲了 Robustness 和 Scalability。

應該把所有的金鑰(AP Keys)都放在硬體加密器裡嗎？

傳統的方法

比較老舊的 HSM 是把所有的金鑰都存放在它裡面，而如果你想備份一把金鑰至另一台 HSM，你必須把兩台 HSM 放在一起方能進行備份。

將金鑰都存放在 HSM 內的缺點

- 金鑰的安全完全仰賴於 HSM，如果沒有備份所有的金鑰，一旦 HSM 因故損壞則受其保護的所有金鑰亦不復見。
- 必須使用另一台 HSM 才能安全地備份金鑰, 如果只是備份到硬碟, 則其程序與安全性堪虞。
- 金鑰的備份與回復會複雜與繁瑣, 每當產生出一把新的金鑰，整個的金鑰複製流程必須再重做一遍。
- HSM 所能夠儲存的金鑰數量完全決定於 HSM 裡安全記憶體的容量，若金鑰的數量超過 HSM 的容量時，只有再買一台昂貴的硬體加密器。
- 當企業成長或對 HSM 需求增加時, 金鑰管理會成爲一個負擔。

「加密金鑰」－Wrapper Keys 的好處

跳脫舊思維－Think (keys) outside the box

有別於傳統式的把金鑰全部存在 HSM 裡，新的思維是只把「加密金鑰」－ wrapper keys 存在 HSM 裡。而用這把「加密金鑰」來加密及加簽於所有的金鑰，把所有被加密的金鑰存放在主機裡，因爲所有的金鑰被「加密金鑰」加密過並以密文的形式存在，只要能保證「加密金鑰」的安全，則可保證所有金鑰的安全無虞。

使用「加密金鑰」－wrapper keys 的好處

- 金鑰複製是一次工程－one time process
  HSM 由於有了「加密金鑰」，它就可以存取任何在主機中受其保護的應用程式金鑰
- 金鑰複製僅需要傳送「加密金鑰」－ wrapper key
  單一的金鑰變得更加容易攜帶與保管 portable
- 只有「加密金鑰」需要被安全地備份
  「加密金鑰」的備份可以被祕密分持而不用花大錢去買多個同樣的硬體加密器，而其他所有的金鑰則可以跟主機裡的資料一起被備份
- 沒有容量的限制
  昂貴的防篡改記憶體僅用來存放「加密金鑰」，而其他的被加密過的金鑰則儲存於硬碟中
- 對安控人員來說，僅需保管「加密金鑰」
  存放在主機內的金鑰可以當做一般的檔案來備份

新舊思維的爭論

有人說：「金鑰存放於硬體加密器外一定不安全…」
我們說：「…但是金鑰是被加密過的，既已加密，又何來不安全之說」
或有人說：「有太多的金鑰備份在磁碟上，很多人都可以拿到…」
我們說：「…但是這些金鑰的備份在沒有『加密金鑰』來解密的情況下是沒用的，而『加密金鑰』則存放在硬體加密器裡並受其保護」
或有人說：「這跟我們以前的作法不一樣…」
我們說：「…但是這個作法與以前的作法相比較熟優熟劣顯而易見!」

你相信加密嗎？

所以，真正的問題是：你相信加密(encryption)嗎?

如果被加密後的金鑰其保密性如同金鑰本身的加密系統甚或過之，那麼，用「加密金鑰」來加密就是安全的。

「加密金鑰」所用的 Triple-DES 加密演算法以目前的科技及可預見的未來都是安全地，而現在還有 AES 可供選擇

金鑰分持、分散風險

俗語云:「不要把所有雞蛋放在同一個籃子裡」!減少內部持有金鑰人員洩密的有效方法就是金鑰分持,把「加密金鑰」分散給多數人持有,並搭配 K-of-N 控管。

何謂 K-of-N 控管?簡言之,設定 N 張卡片,其中任 K 張到齊才行,而 N 大於等於 K;如此一來,便可設定某重要的安全應用程式必得至少有 K 張卡片到齊,方可啓動,達到防止人員洩密的可能。同樣地,K-of-N 控管亦可用做於金鑰備份及回復。

新舊思維的比較

比較項目	所有金鑰都在 HSM 裡	只有最重要的「加密金鑰」在 HSM 裡
金鑰的安全性	很高	很高
備份與回復	很麻煩	容易
金鑰備份安全性	爲了安全備份金鑰,必須多買一台 HSM	很高
可存放的金鑰有數量	有限制	無限制
系統擴充性	有限或麻煩	容易

nCipher Security World

nCipher 的 Security World 是設計來幫助 nCipher HSM 達到對金鑰的產生、使用、管理、儲存及銷毀等功能的重要架構。Security World 可依據客戶的需求及其安全政策來做相應的配置。使用者可透過 GUI 介面的 KeySafe™或是 command line(命令列)模式來達至上述金鑰管理之功能。

Security World 提供了多項的安控機制，除了 k-of-n 的存取控管外，對每張卡片，更可設定一組密碼，以達到更嚴僅的安全控管。

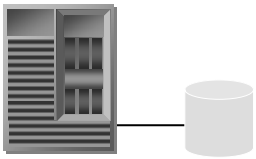
Security World 裡面有四個重要的原素：

(1)HSM－硬體加解密模組

專屬型硬體加解密模組

網路型硬體加解密模組

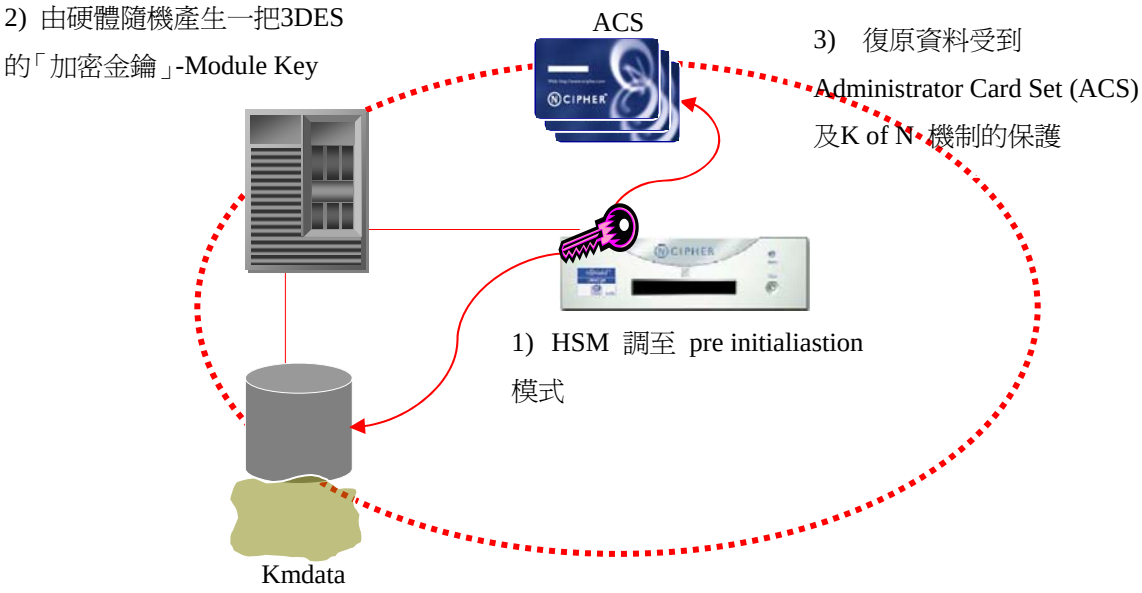
(2)kmdata



(3)ACS: Administrator Card Set

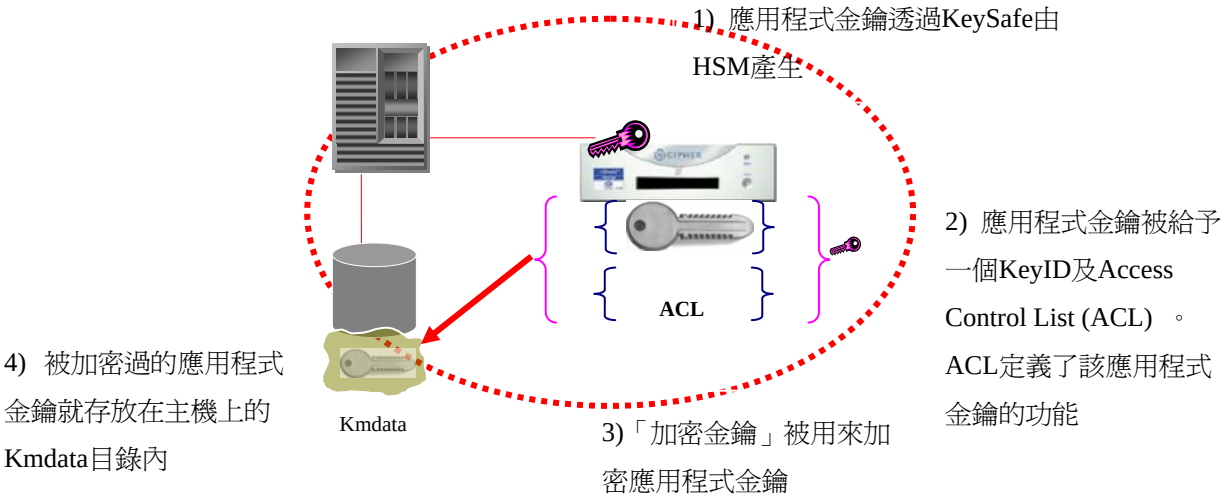
(4) OCS: Operator Card Set

建立 Security World



HSM 必須是在 pre initialiastion mode 才可建立 Security World
ACS 具有 k-of-n 的機制，並可爲每一張卡片都設定密碼來提供多一層的保護

透過「加密金鑰」來保護應用程式的金鑰

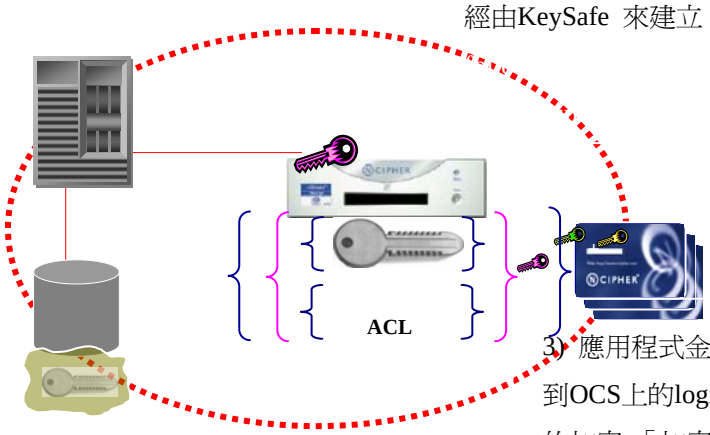


應用程式金鑰除了可透過 KeySafe 從 HSM 來產生外，亦可從外部匯入已經存在的應用程式金鑰，不過，爲了安全的理由，我們不建議這樣做，因爲，只有不爲人知的金鑰才是安全的金鑰

Access Control List (ACL)是 Security World 裡面非常重要的工具，每一把金鑰都有其獨一的 ACL，ACL 裡面定義好的該應用程式金鑰所有的功能及權限

透過 OCS 來保護應用程式的金鑰

1) Operator Card Set (OCS) 經由KeySafe 來建立



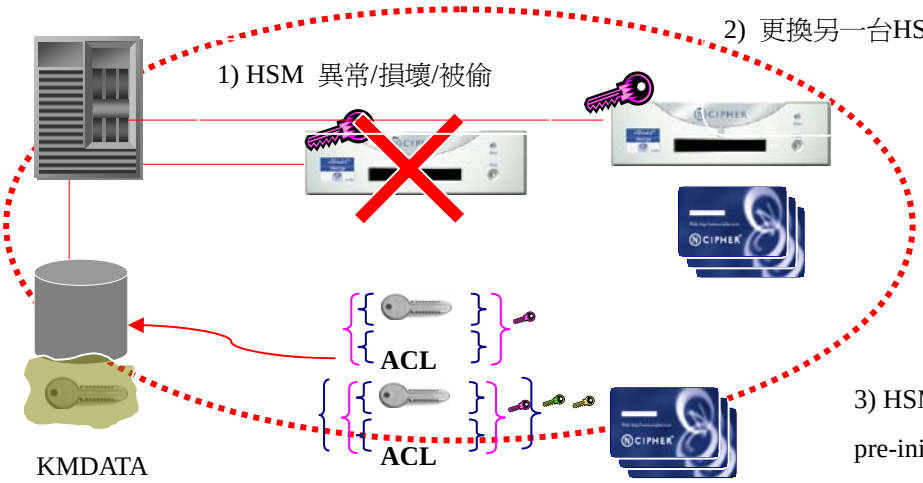
4) 被加密過的應用程式金鑰就存放在主機上的Kmdata目錄內

2) 產生應用程式金鑰並選擇由 Operator Card Set (OCS) 來保護之。應用程式金鑰先被「加密金鑰」加密過

3) 應用程式金鑰接著受到OCS上的logical token的加密，「加密金鑰」接著又用來加密一次

透過 OCS 的保護，某應用程式可以被授權僅予特定的人員來操作，凡非授權人員將無法呼叫與該金鑰相對應的應用程式

災難復原

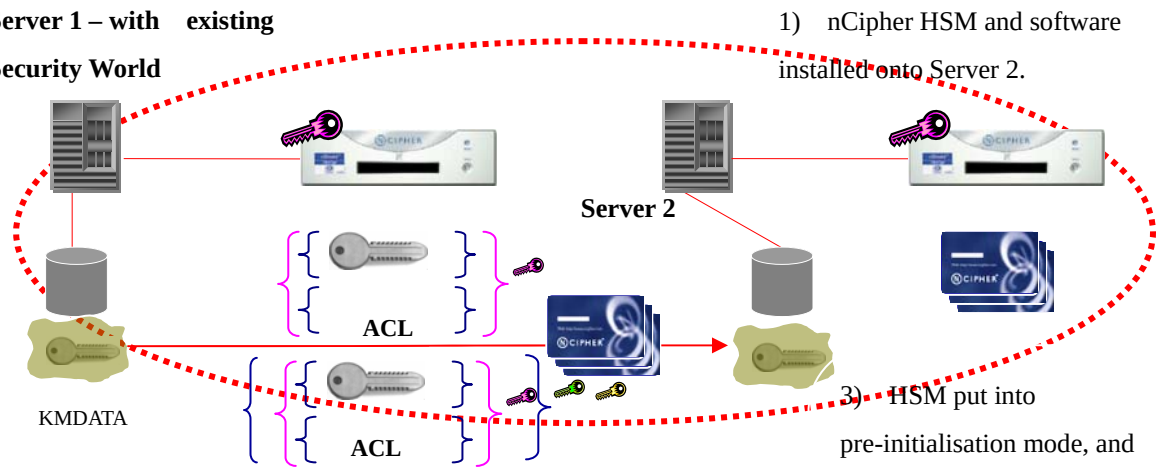


3) HSM 調至 pre-initialisation 模式，然後經由 KeySafe 或 command line－'restore existing security world' 並使用 ACS 從KMDATA目錄來回復 security world

4) HSM 調回至 operational 模式，所有的透過「加密金鑰」及OCS保護的應用程式金鑰又重新受到新的HSM的保護.

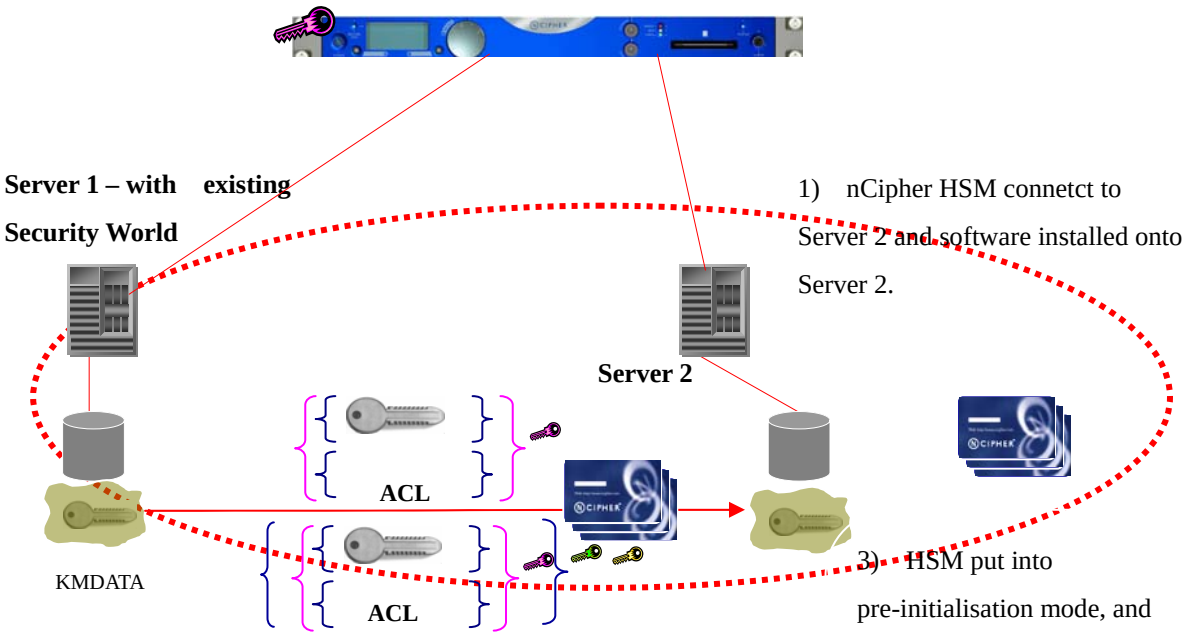
當 HSM 有異常、損壞或是被偷時，僅需將另一台 HSM 接上主機，並將之調至 pre-initialisation mode，然後將至少 f 張的 ACS 卡準備好，透過 KeySafe 或是 command line 就可將 Security World 從 KMDATA 目錄裡回復過來。

單一 Security World 管理多台伺服器上的 HSM



當需要多加一台 HSM 於另一台伺服器上時，僅需先把新的 HSM 安裝至第二台伺服器上，並將第一台伺服器上的 KMDATA 複製至第二台伺服器上，再將第二台 HSM 調至 pre-initialisation mode，並透過 KeySafe 或 command line 來將第二台上的 Security World 啓動。

單一 Security World 與 netHSM 管理多台伺服器



增加一台伺服器至網路型的 HSM 上更容易，不用再買多一台 HSM，只需將第二台伺服器透過網路連至 netHSM 上，其他步驟都相同。

可升級的安全架構

當使用 nCipher Security World 的架構時，可升級的安全架構便變得確實可行，當所有的金鑰都以加密的形式存放在主機裡，而「加密金鑰」存放在「硬體加密器」裡時，由於有「加密金鑰」來做安全上的控管，如此，可進行金鑰的備份而不會安全上的疑慮，而系統本身可視其需要來增加設備以增進效能及穩定性，系統透過單一的「加密金鑰」便可處理許多的應用程式金鑰。

當企業組織的規模擴大，而其所使用的金鑰亦隨之增多時，nCipher Security World 讓企業組織對金鑰的管理仍是那樣的容易。