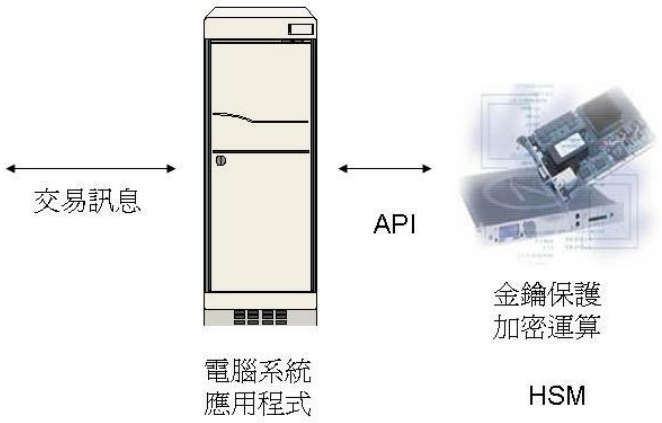
資料安全需要硬體加密設備—nCipher HSM

HSM 是 Hardware Security Module 的縮寫，有譯成「硬體安全模組」，或「硬體加密器」，或「亂碼化設備」.

一串明碼資料經過加密或亂碼(Cryptography)後變成一堆沒有意義的亂碼，資料加密或亂碼化是複雜的運算過程，需要一個或一對金鑰(Key)當輸入值，而演算法是公開的，如果沒有保護好金鑰，如果演算過程暴露在外，絕無安全可言．又因加密運算極耗電腦資源，大量加密資料需求會造成電腦效能下降.

HSM 目的有二

1. 更安全: 使用硬體方式來儲存與保護金鑰，加解密運算(Cryptography)過程都在 HSM 內進行，真正的亂數產生金鑰
2. 提昇運算效能:專屬晶片加解密運算處理，不佔用電腦資源



常見的加密演算法:

1. 對稱式演算法: DES/3DES, AES, RC4…使用同一把金鑰來加密與解密
2. 非對稱式演算法: RSA, DSA…使用一對(公鑰與私鑰)來加密與解密
3. 湊雜函數: MD2/MD2, SHA-1/SHA-2..

HSM 通常會支援下列的業界標準 API:

1. PKCS#11
2. Java JCA/JCE
3. Microsoft CAPI
4. 或者支援公開源始碼 OpenSSL

當然各廠商也會提供專屬的 API，以充分運用該產品的特色.

金鑰管理包括金鑰產生，分送，使用，儲存，銷毀等生命週期的管理，例如最核心的金鑰必須被 HSM 保護好，其它金要也要以安全的方式存放，不可以明碼方式暴露在 HSM 之外.

HSM 的效能

因爲非對稱式加密比對稱式加密要複雜許多 (速度大約 1:1000)，所以 HSM 通常以 RSA 1024 bit 簽章運算能力來代表其效能，單位爲 TPS – Transaction Per Second

HSM 型式

1. 網路型: Network Appliance，可以多台電腦共用
2. PCI/PCI-X: PCI 卡
3. SCSI: 卡片或外接盒子
4. 支援新的 PCI-Express 介面
5. 其它如 USB, PCMCIA, Chip…等小的型式，各有其不同應用領域

HSM 的安全性是依照 NIST 的 FIPS 140 規範的，安全規範共 11 項，又分四個等級:

1. Level 1: 加密模組使用核定演算法，且內部運作不會被窺視到
2. Level 2: Level 1 + 破壞存跡特性
3. Level 3: Level 2 + 破壞偵測與反應特性
4. Level 4: Level 3 + 異常環境偵測

等級越高代表安全要求越高，相對價格也越高，實務上端視安全需求而定.

HSM 應用

舉凡需要用到對稱或非對稱加密運算的應用系統都需要 HSM，例如:

1. PKI: CA 簽發憑證 (Certificates)
2. 電子簽章及其應用
3. 信用卡交易
4. 金融跨行交易
5. 電子時戳, Code Signing,…等等

nCipher HSM 產品線

1. 網路型 HSM: netHSM 500 TPS, 2000 TPS
2. 卡片型 HSM: nShield 500 TPS, 2000 TPS, 4000 TPS, 支援 PCI-Express
3. Mini-HSM: 可供網路安全設備使用

nCipher HSM 特點

1. 取得最多 FIPS 140-2 認證
2. 效能領先同業
3. 領先金鑰管理設計: K of N 金鑰分持，最容易管理: 金鑰備份，回復，擴充…

nCipher HSM 台灣代理商: 玉山科技 http://www.asiapeak.com, (02)77128295