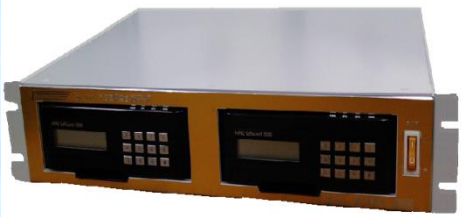
中華電信密碼安全模組(保密器)
（HiPKI SafGuard 1200 HSM ）

TM:A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.



歐美各國對於密碼模組的輸出大都有相當程度的管制措施，並且密碼安全模組的使用可能會影響整個國家的安全，所以建立本土的密碼模組研發技術是非常重要的。中華電信密碼安全模組為我國自行研發的密碼模組裝置，其安全設計已通過國際認可的密碼模組標準 NIST FIPS 140-2 Level 3 驗證，可應用於安全儲存各類伺服器的私密金鑰，以及數位簽章作業的安控單元，能有效強化伺服器的安全性及可信度。

產品特色

1. 鑰控管安全性高

一旦私密金鑰儲存到高速保密器後，所有的加解密運算都是在密碼安全模組中安全地執行，可有效避免私密金鑰遭受竊取。

2. 加解密運算效率佳

設計專用的硬體執行加解密運算，其效能較軟體方式高出甚多，故伺服器軟體可空出時間提供更多且更穩定的服務。

3. 嚴密安控啟動機制

利用安控 IC 卡由主管與作業人員共同控管保密器之啟動，防止非授權之使用。

4. 完全自行研發技術，可依客戶需求進行客製化設計

高速保密器是由中華電信研究所自行研發的產品，掌握完整的技術解決方案，可依客戶的安全需求提供更安全的密碼演算法及不同的金鑰長度。

5. 滿意的產品服務及技術支援

提供詳細的產品中文使用說明文件，以及堅強的專業技術支援人力，可配合客戶進行完整的教育訓練及顧問服務。

產品主要功能

- 已通過國際認可的密碼模組標準 FIPS 140-2 Level 3 的安全規範
- 依安全需求提供 2048、4096 位元等多種的 RSA 金鑰長度選擇。
- 內建真實亂數產生器(Physical RNG)，確保金鑰產生之亂度及品質。
- 具備預防竄改(Tamperproof)的開蓋金鑰銷毀功能。
- 具有開機啟動後自我檢查功能(Boot up self checking)。
- 依存取權限分成安控人員及作業人員兩種角色
- 內建 IC 卡讀寫模組，具備金鑰分持、備份以及安全控管機制。
- 提供主機間的認證及授權存取安全控管。
- 提供安全稽核的事件記錄給稽核伺服器。
- 提供多組金鑰儲存(包含RSA、Triple DES 、 AES、ECC 等)。
- 支援密碼演算法
  - 對稱式 :Triple DES (FIPS certified), AES (FIPS certified)
  - 非對稱： RSA (FIPS certified)
  - 雜湊函數 : SHA-1, SHA-224,SHA-256,SHA-384,SHA-512(FIPS certified)
  - 亂數產生器 : DRBG(FIPS certified)
- 支援API : PKCS#11, Microsoft CSP
- 可搭配使用於中華電信研發的電子閘門、稽核伺服器系統、 On site CA系統、時戳服務及存證服務等系統。
- Web 管理介面，全中文化介面，操作簡易明瞭。
- 具有憑證管理機制，憑證需求檔製作、憑證簽發、與憑證管理。

產品技術規格

1. 演算法 ：
   - ➢ 對稱式 ：
     - ● Triple DES, 3-keyECB and CBC mode (FIPS certified),
       - • Triple DES,執行效能為≧ 300MBits/Sec.
     - ● AES 128/192/256bits, ECB and CBC mode (FIPS certified)
       - • AES 128-bit,執行效能為≧ 960MBits/Sec.
       - • AES 192-bit,執行效能為≧ 800MBits/Sec.
       - • AES 256-bit,執行效能為≧ 685MBits/Sec.
   - ➢ 非對稱 :
     - ● RSA 1024-bit ,簽章效能200次/秒. (RSA 1024: 80 TPS) (FIPS certified)
     - ● RSA 2048-bit ,簽章效能100次/秒. (FIPS certified)
   - ➢ 雜湊函數 :
     - ● SHA-1,執行效能為≧ 320MBits/Sec. (FIPS certified)
     - ● SHA-224,執行效能為≧ 200MBits/Sec. (FIPS certified)
     - ● SHA-256,執行效能為≧ 200MBits/Sec. (FIPS certified)
     - ● SHA-384,執行效能為≧ 320MBits/Sec. (FIPS certified)
     - ● SHA-512,執行效能為≧ 320MBits/Sec. (FIPS certified)
   - ➢ 亂數產生器 :
     DRBG(FIPS certified)

2. 支援 API :
   - ● PKCS#11
   - ● CSP for Microsoft Crypto API
3. RS232控制 IPv4 Ethernet port Enable與IP assign
4. 連接界面：提供Ethernet 10/100Mbps RJ-45 x 4
5. 憑證需求檔符合 pkcs#10，憑證金鑰檔符合 pkcs#12
6. 使用者 Web 管理界面
7. 實體尺寸：約 430 mm (長) x 380 mm (寬) x 90 mm (高)
8. 輸入電壓：AC 110V
9. 工作溫度：18 ~ 28 ℃,
10. 相對溼度：20% ~ 85% 在 25 ℃
11. 認證 :
    ① FCC: CFR47, Part 15, Subpart B, Class B
    ② FIPS 140-2 level 3
12. 生產國家：中華民國
13. 組成套件：
    ① HiPKI SafGuard 1000 HSM SI 一台
    ② 光碟片一片(內含金鑰管理工具、驅動程式、系統程式發展軟體(SDK)和完整的安裝與使用說明書的電子檔案)