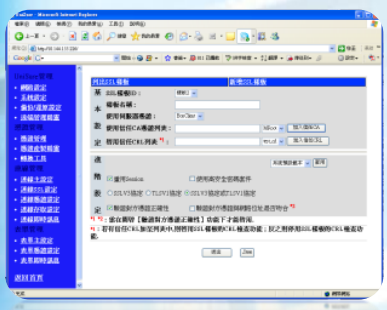
# 安全聯網系統
# (SSL VPN)




本安全系統平台系統架構符合SSL(Secure Socket Layer)/TLS(Transport Layer Security)安全通訊協定，提供網路應用程式在網際網路上做資料傳輸與電子交易所需的安全保護功能。對Client 與Server間傳送的資料提供資料加密(Encryption)資料隱密性及完整性保護。可搭配GCA憑證、與密碼控管等多樣組合，提供驗證機制、繞路轉接授權登入控制機制。同時也針對電子閘門伺服軟體金鑰提供高安全的儲存媒介。

## 產品特色

1. 提供一個安全的通訊環境

安全聯網不僅讓用戶端以應用程式透通(transparency)方式安全轉接，更讓遠處位於轉接系統後的應用程式伺服端安全地接收與發送通訊資料，能夠有效地防止機密資料(sensitive information)在傳送過程中外洩(disclosure)、防止非法人員對傳送資料篡改及防止非法人員冒名傳送假資料，以確保訊息來源身份的辨識。

2. 提供便宜、簡單的解決方案

現今的VPN產品在價格上視其整合性、效能與其他附加功能，且VPN在金鑰管理上的多樣性與複雜性，反而影響到不同品牌，甚至同品牌不同類型VPN產品間的相容性。而系統，使用SSL/TLS的機制，不僅金鑰交換、密鑰產生、與資料加解密皆是由SSL/TLS協定完成，因此安全聯網系統比任何VPN產品皆有價格上的競爭優勢。

3. 採用強化的安全機制

安全聯網系統特地針對SSL/TLS協定上的弱點，作防範與加強，使用AES等安全度較高的對稱式密碼演算法，並且將系統中最重要的私密金鑰寫入硬體中。這些方法皆能有效地增加系統對內對外的安全度，確保系統運作安全無虞。

4. 相容於瀏覽器密碼機制

一般瀏覽器(Browser)皆內建SSL/TLS功能，可以與具備SSL/TLS功能的網頁提供伺服器建立起加密通道，使用者更可以將自己的憑證匯入瀏覽器中，作為遠端網頁提供伺服器確認使用者身份之用。這樣的機制同樣可以轉移到瀏覽器與安全聯網系統，兩者之間不僅可以建立起SSL/TLS加密通道，以確認使用者的真實身份，在確認使用者身份後，再提供使用者安全通訊轉接的功能。

中華電信研究院 資通安全研究所
桃園縣楊梅鎮電研路99號
Tel：+886-3-4245885 Fax：+886-3-4244147
http://www.chttl.com.tw/

# 安全聯網規格

一.　憑證管理：

1. 憑證簽發：簽發伺服器憑證、簽發使用者憑證
2. 憑證需求檔: 英文需求檔、中文需求檔
3. 網路TCP明文轉接功能：SSL轉接SSL，TCP明文轉接和TCP明文與SSL互轉
4. 憑證載入，匯出，管理伺服器憑證，憑證瀏覽中文顯示
5. 憑證需求檔符合 pkcs#10，憑證金鑰檔符合 pkcs#12
6. 系統管理備援機制全中文介面控管
7. 控管介面Browser介面，系統參數備份與載入

二.　連線管理：

1. 網路TCP明文轉接功能，SSL轉接SSL，TCP明文轉接和TCP明文與SSL協定互轉
2. SSL VPN 連線功能
3. 支援SSL單向或雙向認證與訊息加密
4. 最高連線 50 user 以上
5. 管理者、使用者連線事件記錄 (log)
6. 連線失敗原因線上查詢
7. 網路的繞路介接管理，包含TCP/IP、POP、HTTP、SMB、CIFS之規約
8. 非 Web-base 之Client-Server 連線加密
9. 連線閒置時間設定
10. 前置病毒與IRMAS 檢查，未通過無法連線
11. 連線完畢，清除快取記錄

三.　驗證管理：

1. 使用者與伺服器雙向憑證認證
2. 管理者密碼認證
3. 遠端管理者遠端 IP認證
4. 使用者 Radius 認證
5. 提供角色權限控管
6. 行動裝置憑證或 VPN密碼登入

四.　硬體規格：

1. 具備Ethernet 10/100 x 4  RJ45
2. 具備 Serial Uart Port  RS232 x 2
3. CISC (Complex Instruction Set Computers) 2.0 GHz以上 CPU
4. LAN Bypass 具有 Disable/Force/Watch Dog Mode 網路備援
5. Dimension (W x D x H)　430 x 380 x 44 mm (19″/1u)
6. 嵌入式Linux 作業系統

中華電信研究院 資通安全研究所
桃園縣楊梅鎮電研路99號
Tel：+886-3-4245885 Fax：+886-3-4244147
http://www.chttl.com.tw/