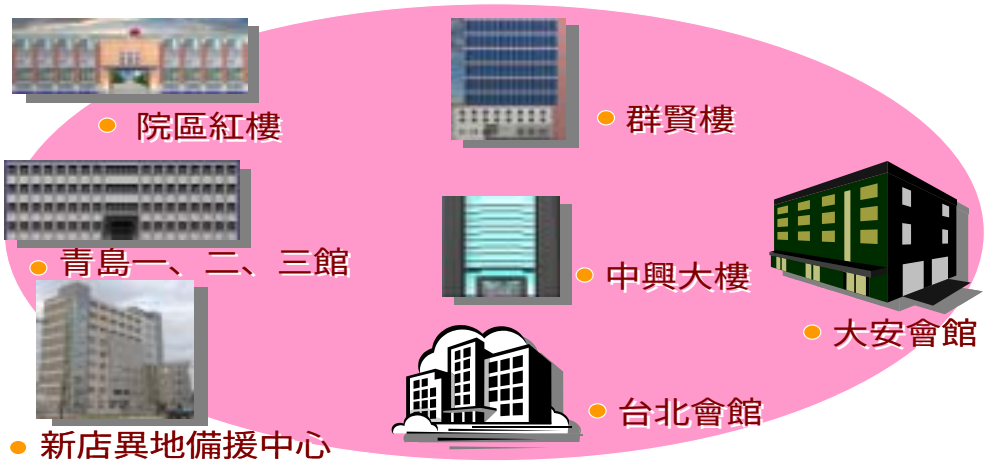
立法院「無線網路系統」介紹

壹、前言

本院爲響應政府「M-Taiwan」計畫，近年來逐步規劃推廣院區的無線網路環境，於 93 年 8 月 31 日完成第一階段無線網路建置案，範圍包含議場、各委員會會議室及中興大樓一樓貴賓室，提供委員於各會議室間能透過無線上網的服務；第二階段於 94 年 12 月 27 日完成全院無線網路環境，範圍包含院區本部、青島第一、二、三會館、群賢樓、委員研究大樓、台北會館、大安會館及新店異地備援中心(圖一)，提供一個移動性的工作環境，使用者可隨時隨地透過筆記型電腦和 PDA 無線上網，對委員於問政和行動化資訊服務工作有所助益，已達成國會全面 M 化之目標。



圖一　立法院無線網路環境示意圖

貳、無線網路建置之考量

本院的網路環境涵蓋範圍廣，院區外圍約 1 公里內，部份委員辦公室以全向性天線無線橋接器方式連線至院區；院區則提供無線基地台連接方式；至於大安會館、台北會館和警察宿舍等外館區域，則藉由雷射傳輸方式連接至院區；茲就本院無線網路建置應用技術之考量說明如下:

一、需形成一個穩定的連線環境:爲使院區範圍沒有無線訊號死角，須對 AP 的位置做良好的規劃，以確保每個 AP 的訊號能有效的重疊。所以，無線網路的現場實地勘測，對無線網路的建置是相當重要的。
二、考慮安全性(須符合 CIA):C 是私密性(confidentiality)、I 是完整性(integrity)、A 是可用性(availability)，故設備本身的安全性，無線網路傳輸空間的安全性及用戶端的安全性須同時確保。
三、使用者身份的確定:以 IC 卡或 Token 經由憑證中心確認使用者身份。
四、無線網路傳輸需加密:傳輸時啓用加密 WEP (Wired Equivalent Privacy)。
五、無線載具的控管:管制無線網路編號(MAC address Locking)使用者需先行註冊，方可使

用。

六、院內私設的無線網路基地台之問題:定期偵測和定位內部非法私設的無線網路基地台，在未來自動以無線或有線的方式去阻擋非法 AP，將連線使用者剔除。

七、適當規劃網段:應將無線網路與內部網路環境分開。

八、無線網路安全方面:須將無線網路使用者加以分類，分別設立防毒閘道清除，甚至阻絕電腦病毒和木馬程式。

九、訂定防火牆的政策:使用者需取得合法授權，方才允許存取。

十、訂定並落實資訊安全政策，定期檢視。

十一、實施電腦資訊教育訓練:針對本院人員實施資訊安全政策和基本電腦防毒教育。

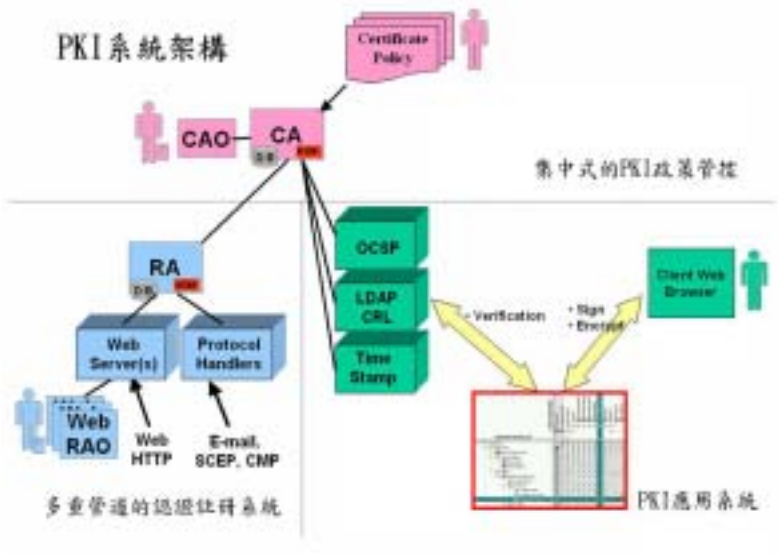
參、無線網路應用及安全技術

本院院內無線網路使用的協定爲 1999 年 IEEE 802.11b 和 2003 年 IEEE802.11g；IEEE802.11b 爲直接序列展頻模式；IEEE802.11g 因相容於 IEEE802.11b 爲雙重展頻模式，兩者均具低輸出功率、低消耗功率、抗雜訊、高頻寬等特點。IEEE802.11b 的傳輸速率 1~11Mbps；IEEE802.11g 的傳輸速率 6~54Mbps、傳輸距離 100 公尺、傳輸角度爲全方向性、可採用 VoIP 技術支援語音傳輸、但易受其他系統的無線電波干擾。

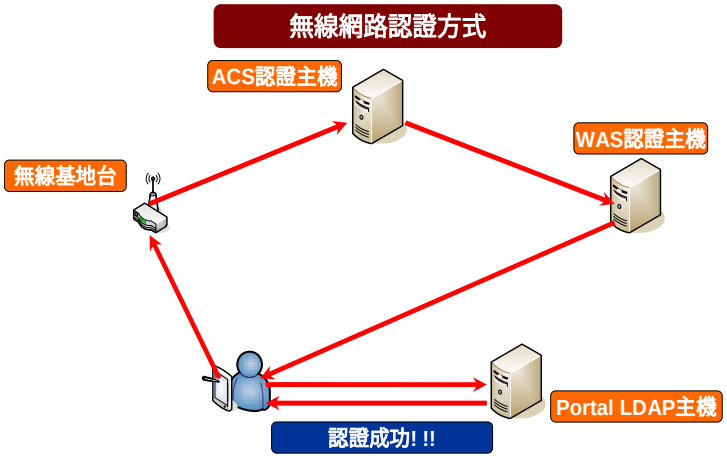
電源方面，院區架設的無線基地台採用 InLine Power 方式，由交換器透過網路線供電。而無線網路的存取點、接取點(Wireless Access Point，簡稱 AP)，會廣播其 SSID(Service Set Identifier)，讓端末裝置可以辨識和偵測是否有服務網路。所謂的 SSID 是 WLAN 的身份名稱。

在 OSI 七層協定中的層層控管方面，考量到無線網路 MAC 存取限制在第二層(Layer 2)爲允許或拒絕 MAC 的服務，而 MAC 爲 6 組 16-bit 的資訊組成，前 3 組是生產業者的身份資訊，後 3 組爲網路產品類型編號和量產號。在 IP 的存取爲第三層(Layer 3)。在 PORT 的存取爲第四層(Layer 4)。HTTPS 中的 HTTP 是 Layer 7，S 是爲 SSL(Secure Socket Layer)是在第六層(Layer 6)。

無線傳輸加密方面，係採用 WEP 方式，是 1997 年 IEEE 802.11 定義下的一種加密方式，就是先在無線 AP 中設定一組金鑰(一般的 AP 通常可設定到四組)，然後無線 AP 會將以此金鑰進行編碼加密，使用者想要連上這個無線 AP 時，就要輸入同樣的金鑰才能連線。



圖二個人電子數位憑證



圖三無線網路認證方式

本院無線網路環境應用公開金鑰基礎建設(Public Key Infrastructure，PKI)並結合了個人電子數位憑證(Digital certificate)(圖二)，並搭配使用無線上網 portal 單一認證機制(圖三)，來提供無線網路方面的服務，以確保資訊安全完整性。並全面控管 NOTEBOOK 和 PDA 之發放使用、權限和核定，以確保合法使用之便利性、即時性及完整性；另建置院區整體網路防駭系統及無線傳輸加密機制，與防制私架無線基地台的統籌管理方法，以確保安全無虞之無線通訊環境。

肆、無線網路應用效益

本院所規劃的無線區域網路環境和無線認證機制，和現有網路認證系統環境整合，並能確實管理、紀錄無線使用者的身份及連線情形。雖然，院區建置防駭及私架無線基地台的管理防制方法，但仍須院內使用者能在資訊安全多加注意，以防資料外洩。

本院所提供的無線網路環境服務，對象除了本院委員、職員、助理外，尚提供各政府機關公務使用，使其能在議場、各委員會議室查詢委員相關的質詢議題，此外，本院在室內和室外環境已能提供 PDA 和手提電腦之網路連線服務，能即時處理各項資訊業務、各委員會議和議場的線上會議內容及院內各資訊應用系統。

目前本院已提供 3G 的 PDA，具有照相功能、藍芽／WiFi 無線傳輸和 GSM 手機功能。此 PDA 如同一部全能小型電腦，可以使委員輕易處理個人資訊、行事曆管理、收發信件、隨時上網即時通訊、照相等。本院並提供網路電話軟體 Skypeout(PDA 版本)之服務，可透過 Skype 打網路電話，以費率較便宜的無線網路，來傳輸語音以及數據資料，未來將加入 GPS 衛星導航功能。

伍、結語

爲推動本院完成的各項電子化和網路化服務系統，本院已建置了無線網路系統基礎環境，以達成”掌握民意脈動、提升服務品質、增進立法時效、建立嶄新國會”的政策目標。雖然，已提供便利的上網環境，但面對無線上網可能遭受到之資訊安全風險日益增高，在資安防護工作上，除賡續強化網路系統基礎建設及防毒防駭功能，定期辦理資訊安全教育訓練和資訊安全政策宣導外，仍有賴於使用者日常作業方面的警覺，以防止個人或公務的資料被有心人士加以利用，才能確保國會資訊安全。

(本文由立法院資訊處資訊助理管理師溫維傑 提供)