

Wireless Security for Hotspots & Home

PCCW

Feb, 2009



Ubiquitous Wireless – Indoor & Outdoor



Wireless Security for Home



- Provides all-in-one DSL modem with Wi-Fi capability to residential customers
- Simplify setup to the general users
- Support WEP/ WPA/ WPA2

End user best practices

Deploy wireless encryption & access control protocols like WPA/ WPA2

Change default password to personalized password

Change network name to something personalized, yet does not reveal location nor owner's name

Stop broadcasting SSID

Move access point away from windows & doors to minimize radio leakage to outdoor

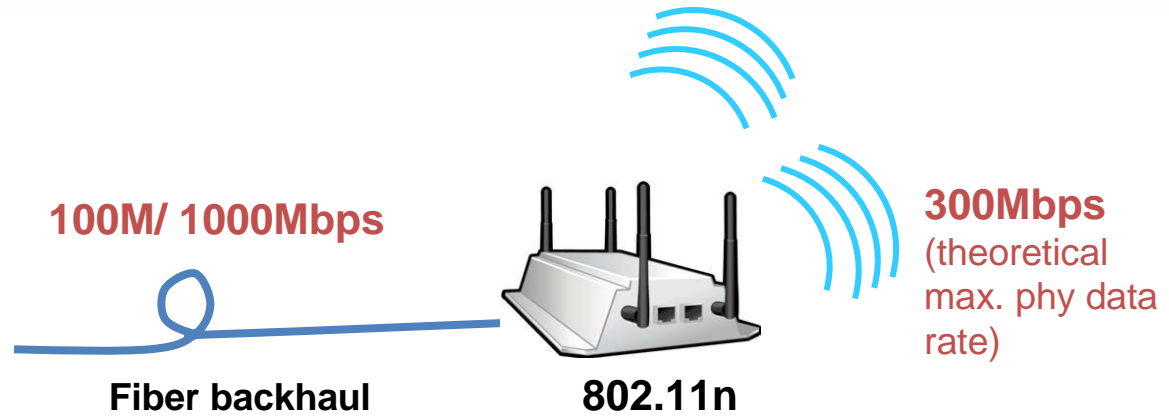


> 5,000 Hotspots

Wi-Fi Usage growth by 16 x since end 2006 !



100M Fiber Hotspot



Super High Speed Hotspot providing over 100Mbps at selected locations with high usage demands



Wireless Security for Mass Market Users

Choice of security solution is a mixed use of the available protocols, compromising the following major factors:

- **Security Vs Usability**
- **Complexity** of solution and **management resources** when serving a large user base
- Capability to offer **support & user training** to the various legacy & advance device models/ OS, with users at different level of IT literacy
- **Throughput & latency** – Layered and strong encryption solutions could be very secure, but the heavy overheads would impair network performance heavily
- Logistics required for **distribution of clients** or certificates to mass market users, if required
- **Cost** of Hardware and Software licenses, while keeping the product cost at affordable level for the mass market consumers
- **Industry acceptance** – sustainable solution/ standards
- **Interoperability** and compatibility with existing network components

➡ **No perfect solution for all**
➡ **Market Education!**



Wireless Security for Mass Market Users

What it takes



Technology

+

**Service Provider
Network Security**

+

End User Practices

OFTA's Guidelines on Wireless Security

First release of “**Guidelines on the Security Aspects for the Design, Implementation, Management and Operation of Public Wi-Fi Service**” was issued by OFTA Oct 2007, after consultation with the industry

- Provides practical guidelines on the security aspects for the **design, technical implementation** (basic & advanced technical measures), **management** and **operation** of public Wi-Fi service with particular emphasis on the air interface
- To promote **user awareness** on the security in using public Wi-Fi services. Operators should provide up-to-date info to users on the capability of their service platforms on wireless security
- Operators should follow the **triggering criteria and reporting procedures** set out in the Guidelines for reporting security violations.



PCCW Hotspot Search Tool

Easy hotspot search tools – prevents users from attaching to Rouge Access Points



無線寬頻熱點
Available here

一見此標誌，即可使用已內置Wi-Fi功能的手提電腦、掌上電腦或其他手提電子產品連接PCCW Wi-Fi寬頻上網，享受穩定流暢的無線上網新體驗！

位置	地址	狀況
1 銅鑼灣港鐵站	銅鑼灣港鐵站上層通道	
2 銅鑼灣港鐵站	銅鑼灣港鐵站上層1號月台	
3 銅鑼灣港鐵站	銅鑼灣港鐵站上層月台	
4 銅鑼灣港鐵站	銅鑼灣港鐵站下層通道	
5 銅鑼灣港鐵站	銅鑼灣港鐵站下層2號月台	

PCCW Wi-Fi寬頻熱點搜尋

香港島
銅鑼灣
全部

*支援802.1x認證

PCCW Wi-Fi一機無限

Google Maps 熱點搜尋

Google Maps 熱點搜尋

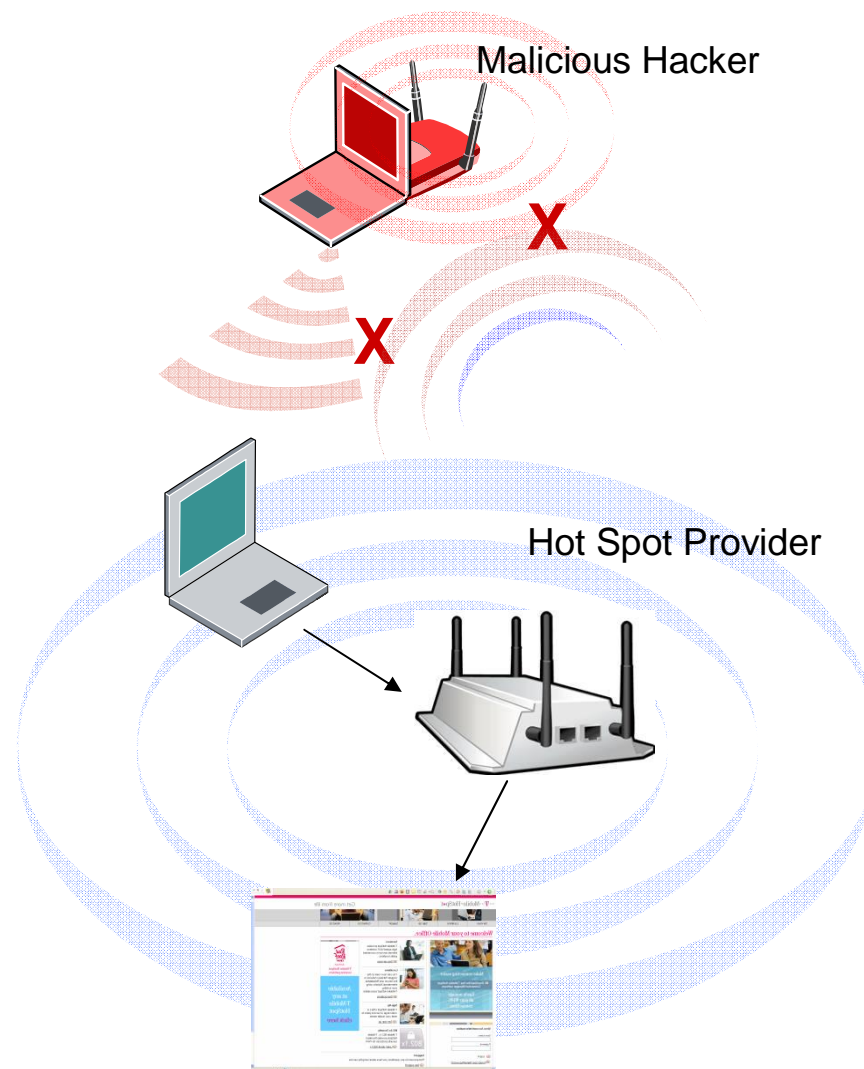
PCCW Wi-Fi寬頻熱點數目不斷增加，現時全港已有超過5,000個無線寬頻熱點。全新「Google Maps熱點搜尋」為你清楚顯示所有熱點於地圖上，位置一目了然，搜尋熱點更快更易。

[搜尋熱點地圖](#)



Service Provider Network Security

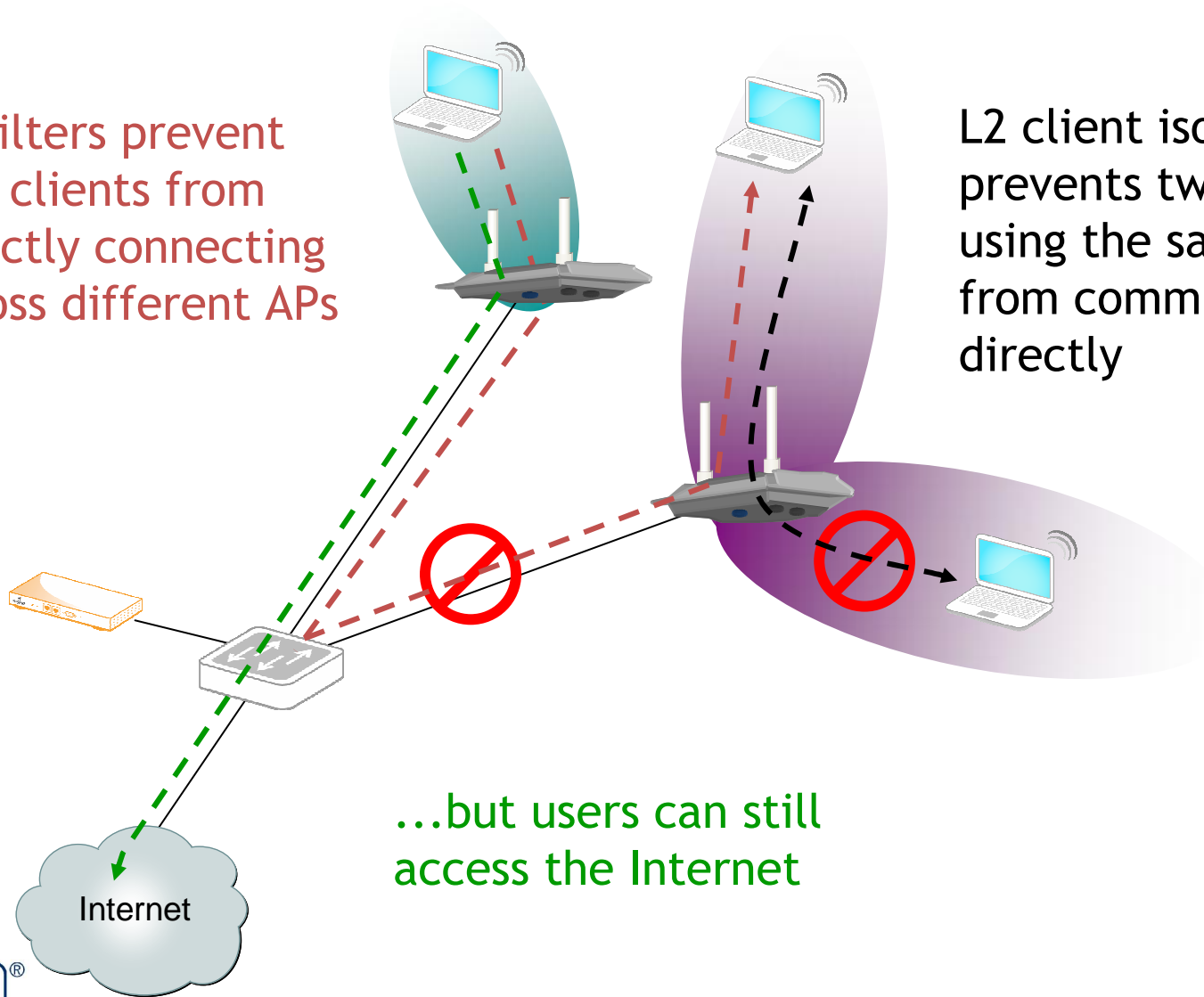
- **Firewall**
 - Screening (flooding) protection
 - Service blocking available for inbound & outbound traffic
 - Active/Passive Mode
- **Intrusion Detection & Prevention**
 - Inbound and outbound traffic with detecting and logging any suspicious activities and network attack
 - Stopping the improper use & notification
- **Wireless encryption**
- **User Authentication**
- **Usage log database**
- **Client isolation**



Service Provider Network Security

L3 filters prevent two clients from directly connecting across different APs

L2 client isolation prevents two clients using the same AP from communicating directly



...but users can still access the Internet

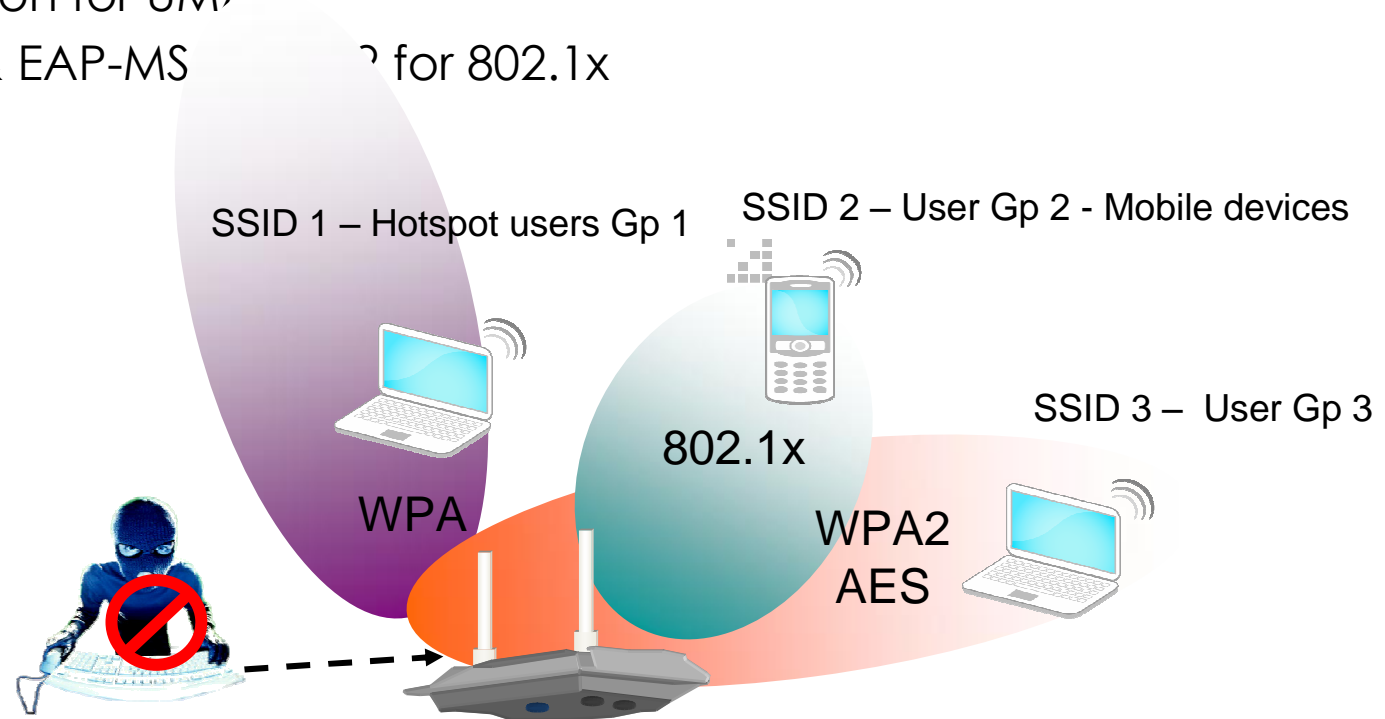
Strategy for Security & Access Control

Providing OPTIONS to suit the varying requirements from different class of users and types of devices

- Users have choice to deploy more secured settings Vs easier to access

UMA and 802.1x Co-exist in Hotspot Environment

- Advertising both SSIDs for UMA (captive portal) & 802.1x
- SSL protection for UMA
- EAP-PEAP & EAP-MS for 802.1x



Security for AirPath



User Login – PCCW Wi-Fi Monthly Plan & Pay-As-You-Go Users

Login ID: @

Password:

Extra Shield by PCCW

- VPN by PPTP for Windows 2000
- WPA/WPA2 with MD5 Encryption for Windows XP, Vista, Windows Mobile 5/6.1 and Symbian S60

* For company domain using Business NETVIGTOR email service ONLY.

✓ Extra-Shield



Our system automatically selects the best possible secure login mechanism for your device, so you can enjoy a hassle-free wireless experience.

Login

Back

For Windows Vista/ XP/ 2000 & Internet Explorer 6 or above only



Extra-Shield

PPTP

Virtual Private Network connection being created automatically during the first time login

Virtual Private Network



Virtual Private Network connection being establish automatically between client PC & PCCW WiFi's VPN server



Extra-Shield

- **802.1x / EAP (Extensible Authentication Protocol)**
 - ‘Dynamic WEP’ - New key per user per session, and updated periodically during a user’s session
 - 802.1x - Users are identified by individual user credentials than hardware profiles, like MAC address
 - Port-based access control
 - SIM authentication for NETVIGATOR Everywhere and selected applications on mobile
 - EAP is a flexible Layer 2 authentication protocol



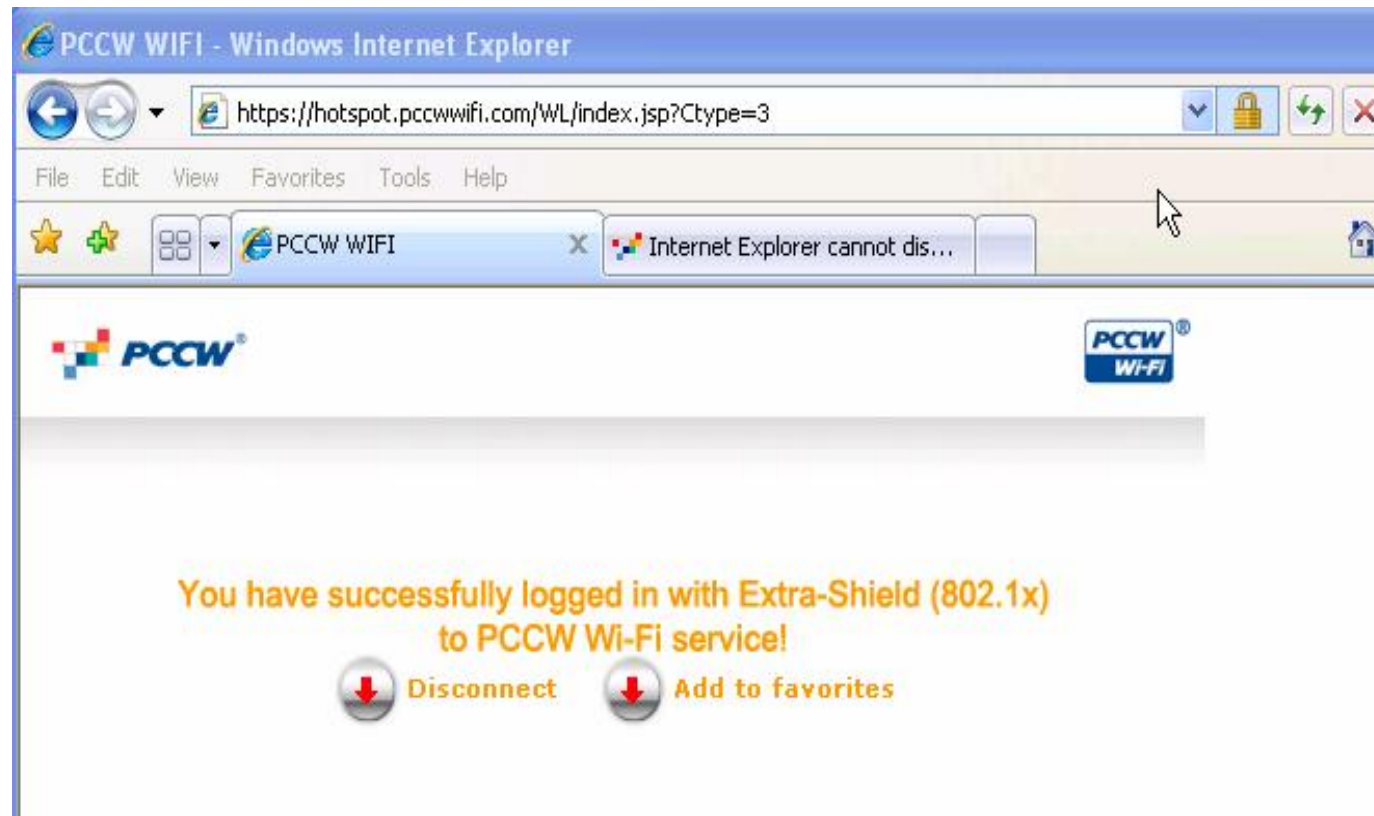
Extra-Shield

802.1x security connection setup on XP, Vista

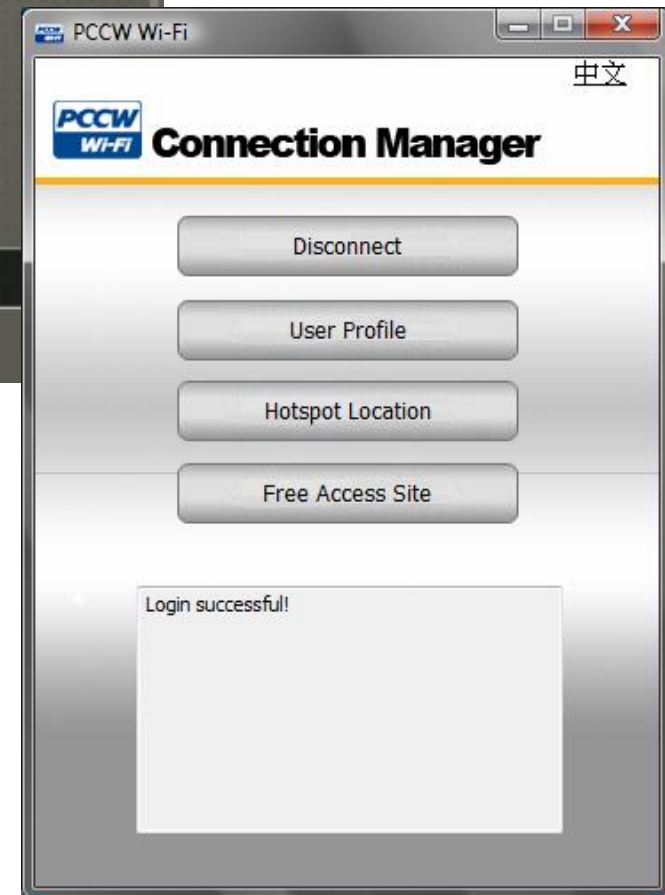
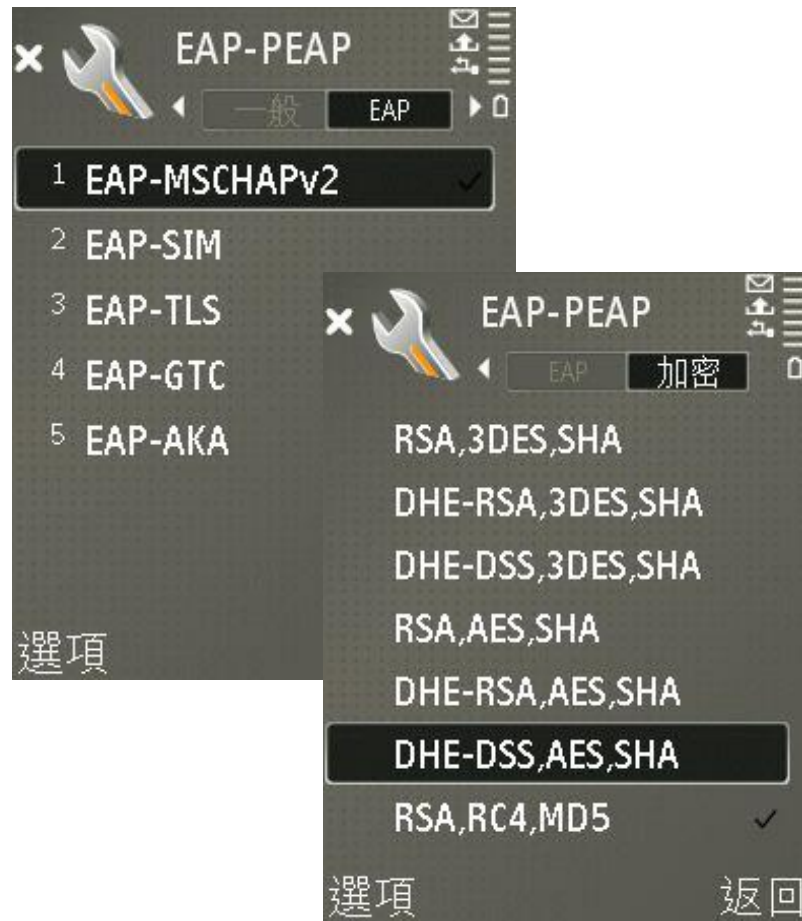
The image displays four overlapping Windows XP network configuration windows:

- 無線網路內容 (Wireless Network Content):** Shows network name (SSID) as PCCW1x and network security type as WPA.
- 無線網路內容 (Wireless Network Content):** Shows EAP type set to Protected EAP (PEAP) and the option "當電腦資訊可用時驗證為電腦" (Authenticate as computer when computer information is available) checked.
- 受保護的 EAP 內容 (Protected EAP Content):** Shows "連線時" (When connected) with "確認伺服器憑證" (Verify server certificate) checked. The list of trusted certificates includes "Thawte Premium Server CA" which is selected.
- 輸入認證 (Enter Credentials):** A dialog box for entering user credentials with "使用者名稱" (Username) as pccw and "密碼" (Password) as ****.

Extra-Shield



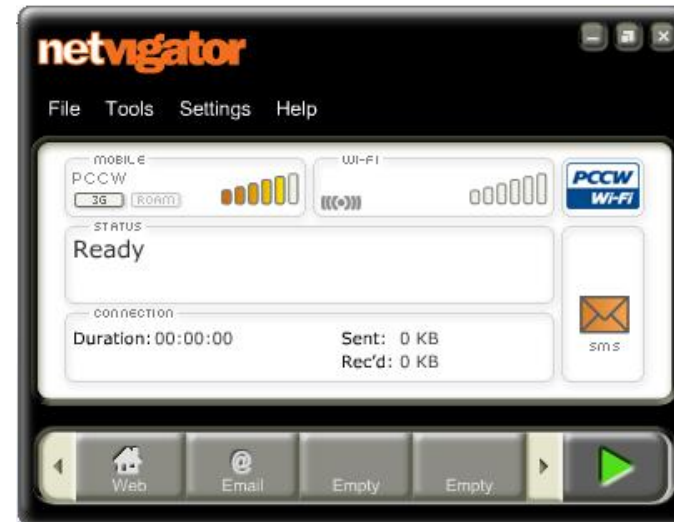
802.1x Connection Manager for Mobile



Support for WM 5/ 6.1 & Symbian S60



802.1x on NETVIGATOR Everywhere



- A unique wireless broadband solution

Wi-Fi + HSPA + 3G

Auto-detects the best network

Authentication by 802.1x EAP-SIM

How to Protect Yourself on Public Hotspots

Customer Education

When you're using an unsecured wireless network, such as a hotspot in a hotel, cafe, or any other public location, you should take steps to make sure your sensitive information isn't exposed:

- **Secure Your Real-time Traffic**
 - Use a VPN connection.
 - Make sure any services you use, such as POP3 and FTP, are secured if you are not using a VPN.
 - Don't visit any private or sensitive Web site unless it's secured (for example, implementing SSL) if you are not using a VPN.
- **Prevent Others from Connecting to Your Laptop**
 - Disable any sharing of files, folders and services.
 - Use personal firewall software.
 - Make sure your operating system is kept up to date.





THANK YOU

Reference: www.pccwwireless.com

