# Wi-Fi Protected Access

**Wi-Fi Protected Access** (**WPA**) and **Wi-Fi Protected Access II** (**WPA2**) are two security protocols and security certification programs developed by the [Wi-Fi Alliance](http://en.wikipedia.org/wiki/Wi-Fi_Alliance) to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, [WEP (Wired Equivalent Privacy)](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy).

WPA (sometimes referred to as the *draft IEEE 802.11i* standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i (or [IEEE 802.11i-2004](http://en.wikipedia.org/wiki/IEEE_802.11i-2004)) standard.

A flaw in a feature added to [Wi-Fi](http://en.wikipedia.org/wiki/Wi-Fi), called [Wi-Fi Protected Setup](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup), allows WPA and WPA2 security to be bypassed and effectively broken in many situations. WPA and WPA2 security implemented without using the Wi-Fi Protected Setup feature are unaffected by the security vulnerability.

## WPA

The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full [IEEE 802.11i](http://en.wikipedia.org/wiki/IEEE_802.11i-2004) standard. WPA could be implemented through [firmware](http://en.wikipedia.org/wiki/Firmware) upgrades on [wireless network interface cards](http://en.wikipedia.org/wiki/Wireless_network_interface_card) designed for WEP that began shipping as far back as 1999. However, since the changes required in the [wireless access points](http://en.wikipedia.org/wiki/Wireless_access_point) (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA.

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the [Temporal Key Integrity Protocol](http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol) (TKIP), was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the [cyclic redundancy check](http://en.wikipedia.org/wiki/Cyclic_redundancy_check) (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled. Well tested [message authentication codes](http://en.wikipedia.org/wiki/Message_authentication_code) existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called [*Michael*](http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#Beck-Tews_attack) to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the key stream from short packets to use for re-injection and [spoofing](http://en.wikipedia.org/wiki/Spoofing_attack).

## WPA2

WPA2 has replaced WPA. WPA2, which requires testing and certification by the Wi-Fi Alliance, implements the mandatory elements of IEEE 802.11i. In particular, it introduces [CCMP](http://en.wikipedia.org/wiki/CCMP), a new [AES](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)-based encryption mode with strong security. Certification began in September, 2004; from March 13, 2006, WPA2 certification is mandatory for all new devices to bear the Wi-Fi trademark.

## Hardware support

WPA was specifically designed to work with wireless hardware that was produced prior to the introduction of the WPA protocol which had only supported inadequate security through [WEP](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy). Some of these devices support the security protocol only after a [firmware](http://en.wikipedia.org/wiki/Firmware) upgrade. Firmware upgrades are not available for some legacy devices.

Wi-Fi devices certified since 2006 support both the WPA and WPA2 security protocols. WPA2 may not work with some older network cards.

## Security

[Pre-shared key](http://en.wikipedia.org/wiki/Pre-shared_key) mode (PSK, also known as *Personal* mode) is designed for home and small office networks that don't require the complexity of an [802.1X](http://en.wikipedia.org/wiki/802.1X) authentication server. Each wireless network device encrypts the network traffic using a 256 bit [key](http://en.wikipedia.org/wiki/Key_(cryptography)). This key may be entered either as a string of 64 [hexadecimal](http://en.wikipedia.org/wiki/Hexadecimal) digits, or as a [passphrase](http://en.wikipedia.org/wiki/Passphrase) of 8 to 63 [printable ASCII characters](http://en.wikipedia.org/wiki/ASCII#ASCII_printable_characters). If ASCII characters are used, the 256 bit key is calculated by applying the [PBKDF2](http://en.wikipedia.org/wiki/PBKDF2) [key derivation function](http://en.wikipedia.org/wiki/Key_derivation_function) to the passphrase, using the [SSID](http://en.wikipedia.org/wiki/SSID#Service_set_identification_.28SSID.29) as the [salt](http://en.wikipedia.org/wiki/Salt_(cryptography)) and 4096 iterations of [HMAC](http://en.wikipedia.org/wiki/HMAC)-[SHA1](http://en.wikipedia.org/wiki/SHA1).

## WPA terminology

Different WPA versions and protection mechanisms can be distinguished based on the version of WPA, the target end-user (according to the method of authentication key distribution), and the encryption protocol used.

### Version

**WPA:** Initial WPA version, to supply enhanced security over the older WEP protocol. Typically uses the TKIP encryption protocol.

**WPA2:** Also known as *IEEE 802.11i-2004*, is the successor of WPA, adds support for CCMP which is intended to replace TKIP encryption protocol. Mandatory for Wi-Fi–certified devices since 2006.

### Target users (authentication key distribution)

**WPA-Personal:** Also referred to as *WPA-PSK* (Pre-shared key) mode, it is designed for home and small office networks and doesn't require an authentication server. Each wireless network device authenticates with the access point using the same 256-bit key generated from a password or passphrase.

**WPA-Enterprise:** Also referred to as *WPA-802.1X mode*, and sometimes just *WPA* (as opposed to WPA-PSK). It is designed for enterprise networks and requires a [RADIUS](http://en.wikipedia.org/wiki/RADIUS) authentication server. This requires a more complicated setup, but provides additional security (e.g. protection against dictionary attacks on short passwords). An Extensible Authentication Protocol (EAP) is used for authentication, which comes in different flavors.

Note that the WPA-Personal and WPA-Enterprise modes are available with both WPA and WPA2.

[**Wi-Fi Protected Setup**](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup)

An alternative authentication key distribution method intended to simplify and strengthen the process, but which, as widely implemented, creates a major security hole (see above).

### Encryption protocol

[**TKIP**](http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol)**(Temporal Key Integrity Protocol):** The [RC4](http://en.wikipedia.org/wiki/RC4) stream cipher is used with a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet. Used by WPA.

[**CCMP**](http://en.wikipedia.org/wiki/CCMP)**:**An AES-based encryption mechanism that is stronger than TKIP. Used by WPA2. Among informal names are "AES" and "AES-CCMP". According to the 802.11n specification, this encryption protocol must be used to achieve the fast [802.11n high bitrate schemes](http://en.wikipedia.org/wiki/IEEE_802.11n-2009#Data_rates), though not all implementations enforce this. Otherwise, the data rate will not exceed 54 MBit/s.

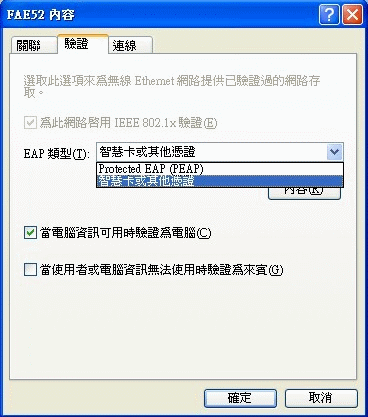
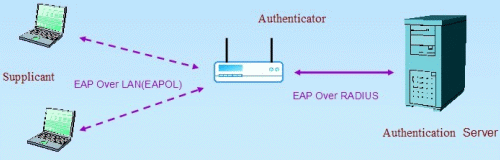
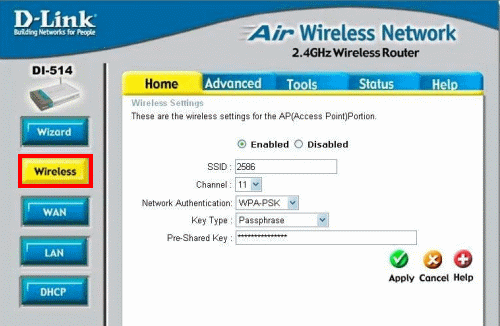
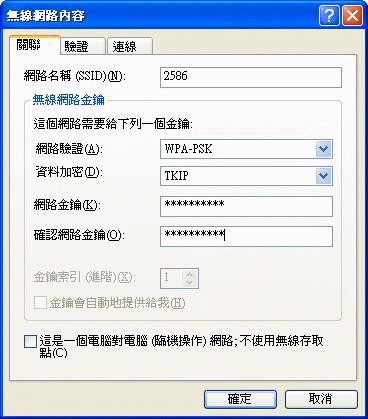
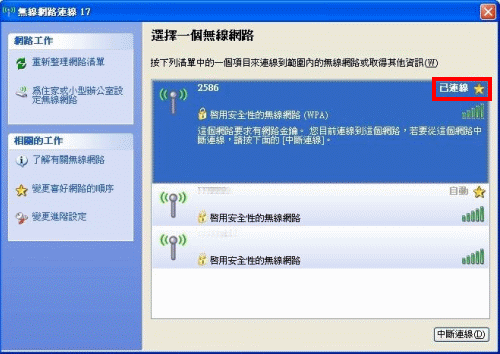
## EAP extensions under WPA and WPA2 Enterprise

In April 2010, the Wi-Fi alliance announced the inclusion of additional [Extensible Authentication Protocol](http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol) (EAP) types to its certification programs for WPA- and WPA2- Enterprise certification programs. This was to ensure that WPA-Enterprise certified products can interoperate with one another. Previously, only EAP-TLS ([Transport Layer Security](http://en.wikipedia.org/wiki/Transport_Layer_Security)) was certified by the Wi-Fi alliance. As of 2010 the certification program includes the following EAP types:

* [EAP-TLS](http://en.wikipedia.org/wiki/EAP-TLS) (previously tested)
* [EAP-TTLS](http://en.wikipedia.org/wiki/EAP-TTLS)/MSCHAPv2 (April 2005 [[24]](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#cite_note-24))
* [PEAPv](http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol)0/EAP-MSCHAPv2 (April 2005)
* PEAPv1/EAP-GTC (April 2005)
* PEAP-TLS
* [EAP-SIM](http://en.wikipedia.org/wiki/EAP-SIM) (April 2005)
* [EAP-AKA](http://en.wikipedia.org/wiki/EAP-AKA) (April 2009 [[25]](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access#cite_note-25))
* [EAP-FAST](http://en.wikipedia.org/wiki/EAP-FAST) (April 2009)

802.1X clients and servers developed by specific firms may support other EAP types. This certification is an attempt for popular EAP types to interoperate; their failure to do so as of 2013 is one of the major issues preventing rollout of 802.1X on heterogeneous networks.

Commercial 802.1X servers include Microsoft [Internet Authentication Service](http://en.wikipedia.org/wiki/Internet_Authentication_Service) and [Juniper Networks](http://en.wikipedia.org/wiki/Juniper_Networks) Steelbelted RADIUS. [FreeRADIUS](http://en.wikipedia.org/wiki/FreeRADIUS" \o "FreeRADIUS) is an open source 802.1X server

**一、前言**  
WPA 無線安全是為針對802.11安全漏洞所提出的一種無線安全過渡解決方案，這些安全漏洞包括缺乏認證機制與 WEP(Wired Equivalency Privacy)加密的缺點。以網路驗證機制而言802.11有「開放系統」與「共用金鑰」這兩種方式，但是「開放系統」沒有任何安全性可言，而「共用金鑰」也因為以明碼方式傳送挑戰本文(Challenge Text)，反而因WEP密鑰的暴露而更不安全，至於 WEP 的加密問題，姑且不談其加密方式已被破解的問題，單單就金鑰的管理，金鑰設定的一致性就可以發現有相當的不方便，若要用於企業環境著實令人擔心。  
**二、WPA安全特性**  
要說明WPA最簡潔的方式就是以WPA = 802.1x + EAP + TKIP + MIC這個「公式」來表示。802.1x與EAP(Extensible Authentication Protocol，延伸驗證協定)是WPA身分驗證的基礎，EAP是實際用來作為 802.1x 驗證的方法。因為是延伸驗證所以可以作到使用者層級，至於驗證的類型有很多種，就 Windows 無線網路支援而言，包括支援憑證與智慧卡驗證的 EAP-TLS (EAP -Transport Layer Security)，與支援密碼驗證作業的Protected-EAP-Microsoft Challenge Handshake Authentication Protocol (PEAP-MS-CHAP v2)。  
  
TKIP(Temporal Key Integrity Protocol，暫時密鑰完整性協定)是WPA用來取代 WEP 的資料加密方法，以動態方式產生及交換金鑰取代了WEP的單一靜態金鑰，每一個封包的金鑰都不一樣，因此安全性大幅改善；至於8位元組的MIC(Message Integrity Protocol，訊息完整性編碼)則取代802.11中的ICV(Integrity Check Value，完整性檢查值)以防止攻擊者攔截、更改甚至重送資料封包，確保資料的完整性。當接收端與傳送端計算出來的MIC值不符時，表示資料遭竄改，該封包即被丟棄。  
**三、支援 WPA 所需的條件**  
由於WPA必須使用到IEEE802.1x，因此必須架設作為帳號認證的認證伺服器(Authentication Server)，例如微軟的ISA (Internet Authentication Service) 伺服器用來管理用戶認證與授權，實際應用上通常會另外架設AD伺服器作為帳號認證的資料庫，AD 伺服器可以與IAS 伺服器裝在同一台機器上，也可以分開架設。  
  
支援 WPA 的無線基地台，角色其實只是很單純地轉送無線用戶端與認證伺服器之間的封包傳遞，一般而言無線基地台可以透過韌體升級來支援 WPA。關於無線用戶端，必須具有處理 WPA 資訊能力的無線網路卡與驅動程式，驅動程式一樣可以透過更新來達成。至於無線用戶端所使用的作業系統，如果使用的作業系統是 Windows XP SP2 或 Windows Server 2003，那您只需啟用 Windows 內建的 Wireles Zero Configuration service，即可以支援 WPA；如果作業系統是 Windows 2000 或是 Windows XP/Windows Server 2003 但不打算使用 Windows 內建的Wireless Zero Configuration service，那您就必須安裝符合 WPA 的無線網路卡設定公用程式。  
**四、WPA 的 SOHO 解決方案**  
對於企業體而言 WPA 的無線安全方案，是必然的解決方案之一，但是對於一般家庭應用卻又顯得不切實際，因為不論架設 AD 或 IAS 伺服器都不是一件小工程，況且家庭數位資料並無企業相對的重要性，因而 WPA 的需要另一套替代方案。WPA-PSK (Pre-Shared Key) 不需要驗證伺服器，使用單一字母數字型式的密碼，不像 WEP 有四組的密鑰選項，設定比WEP簡單安全且具有一致性，比較適合 SOHO 用戶環境使用。然而在共享密鑰的設定上仍需考慮應有的長度與複雜性，以避免密鑰被破解的危險。  
  
**五、WPA-PSK 實例應用**  
  
**《步驟1》** WPA-PSK 的設定很容易，我們以 D-Link DI-514 無線路由器作為範例。首先進入 DI-514 設定畫面，選擇 Wireless 選單，選填 SSID (Service Set Identification) 與 Channel 之後，最主要在 Network Authentication 項目選擇「WPA-PSK」，並且在 Pre-Shared Key 欄位輸入一組金鑰並且把它記下來。  
  
  
  
  
**《步驟2》**接著在無線用戶端，請開啟無線網路內容再新增一組設定，同樣地在網路驗證選項選擇 WPA-PSK，並且把先前 AP Router 設定紀錄下來的密鑰，在網路金鑰欄位照樣輸入。以上設定必須與 AP Router設定相符合，關於網路金鑰設定必需 8~63 個 ASCII 字元或 64 個 16 進位字元，應有一定的複雜性以避免被暴力破解法突破。  
  
  
  
  
**《步驟3》**確定設定無誤之後，我們檢視連線後的畫面(Windows XP SP2)，右上角顯示「已連線」，表示已經正常連線。  
  
  
  
  
WPA 是目前無線網路安全的一種過渡解決方案，但最終的解決還是要等IEEE802.11i 產品的普及，對於 IEEE802.11i 的標準而言，WPA 已被涵蓋在其規範之中。目前市面上已有越來越多的無線產品開始支援 WPA，足以作為無線網路安全的替代方案。