



## Overview

### Wi-Fi Protected Access for the Home

Over the past year, many Wi-Fi Alliance members and their customers have become increasingly concerned about the vulnerabilities of Wired Equivalent Privacy (WEP), the security mechanism included in Wi-Fi CERTIFIED products to date. In response, the Wi-Fi Alliance, in conjunction with the IEEE, has driven an effort to bring strongly improved, interoperable Wi-Fi security to market in the first quarter of 2003. The result of that effort is Wi-Fi Protected Access.

Wi-Fi Protected Access is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Wi-Fi Protected Access is designed to run on existing hardware as a software upgrade. Wi-Fi Protected Access is derived from the upcoming IEEE 802.11i standard and will be forward-compatible with it. Wi-Fi Protected Access, when properly installed, will provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network.

Wi-Fi Protected Access is useful for both large business deployment and for more casual home use, though this paper will focus on Wi-Fi Protected Access in a home environment.

Security requirements vary depending on the amount of network traffic and the level of secrecy required for the information being exchanged and the applications being used. While professional users typically require enterprise-quality security to allow secure conduct of confidential business, the security requirements of casual low-volume home users, using their network to print or share files, surf the Internet or exchange email with friends and family, tend to be less stringent. Wi-Fi Protected Access is designed to meet these different requirements by running in two different modes – enterprise and home mode. In enterprise mode, a network server and sophisticated authentication mechanisms are utilized and automatically distribute special encryption keys, called master keys.

In a home environment, where there are no network servers, Wi-Fi Protected Access runs in a special mode, which allows the use of manually entered keys or passwords instead. This mode, also called Pre-Shared Key (PSK), is designed to be easy to set up for the home user. All the home user needs to do is enter a password (also called a master key) into their access point or home wireless gateway and each PC that is on the Wi-Fi wireless network. After entering the password, Wi-Fi Protected Access automatically takes over. First, it keeps out eavesdroppers and other unauthorized users by requiring all devices to have the matching password. Second, the password kicks off the encryption process, which in Wi-Fi Protected Access is called Temporal Key Integrity Protocol (TKIP).

This is where the mechanics of Wi-Fi Protected Access are substantially different from WEP, where the same static encryption key is used over and over again. TKIP takes the original master key only as a starting point and derives its encryption keys mathematically from this master key. TKIP then regularly changes and rotates the

encryption keys so that the same encryption key is never used twice. This all happens in the background automatically, invisible to the user. Together, these features make Wi-Fi Protected Access a far stronger security solution than WEP.

While no security mechanism can be considered “absolutely secure,” the protection given by Wi-Fi Protected Access in PSK mode is strong enough to prevent most attacks, even sophisticated ones. As such, Wi-Fi Protected Access offers a pragmatic, economical security mechanism for most home users.

It is worth mentioning that telecommuters and other professionals, while they may be physically working from home, may have more stringent enterprise-class security requirements, which may be more than Wi-Fi Protected Access in home mode can offer. It is recommended that these users consult with their IT administrator for details.

A useful benefit of Wi-Fi Protected Access is that it is designed to be software upgradeable for existing Wi-Fi CERTIFIED products, which means that in most cases, existing products will not need to be replaced. So, if you are already using Wi-Fi CERTIFIED products, your product vendor may be able to send you the appropriate software upgrade. If you are looking for new Wi-Fi products, look for products that are both Wi-Fi CERTIFIED (displaying the Wi-Fi logo) and include Wi-Fi Protected Access.

In summary, Wi-Fi Protected Access is designed to meet the requirements of both large business users and the typical home user. The PSK home mode of operation of Wi-Fi Protected Access offers greatly strengthened security over WEP, and has been specifically designed for home users. The Wi-Fi Alliance plans to begin interoperability certification testing on Wi-Fi Protected Access starting in February 2003.

Press and analyst contact:  
Robert Durand  
Edelman  
512.478.3335  
robert.durand@edelman.com

Michael Diamond  
Edelman  
650.429.2772  
michael.diamond@edelman.com

rev. 10/18/2005