



Q&A

Wi-Fi Protected Access™

1. Q: What is Wi-Fi Protected Access?

A: Wi-Fi Protected Access is a specification of standards-based, interoperable security enhancements, which strongly increase the level of data protection (encryption) and access control (authentication) for existing and future Wi-Fi wireless LAN systems.

2. Q: How long will Wi-Fi Protected Access be an effective security solution?

A: Wi-Fi Protected Access will be deployed starting in early 2003 and will be viable for many years to come.

3. Q: Is Wi-Fi Protected Access an IEEE 802.11 standard?

A: No, but it is based on an IEEE 802.11 standard. Wi-Fi Protected Access is derived from the forthcoming IEEE 802.11i draft standard and is designed to be forward-compatible with that standard when it is published.

4. Q: How did Wi-Fi Protected Access come into being?

A: Wi-Fi's original security mechanism, Wired Equivalent Privacy (WEP), has been viewed as insufficient for securing confidential business communications. A longer term solution, the IEEE 802.11i standard, is under development. However, since the IEEE 802.11i standard is not expected to be published until the end of 2003, several members of the Wi-Fi Alliance teamed up with members of the IEEE 802.11i task group to develop a significant near-term enhancement to Wi-Fi security. Together, this team developed Wi-Fi Protected Access.

The effort was also driven by the need for enhanced Wi-Fi security that would be software-upgradeable to the more than 650 Wi-Fi CERTIFIED products in existence today. Wi-Fi Protected Access is designed to be a software upgrade, whereas obtaining all of the advantages of the full IEEE 802.11i standard will likely require a hardware change.

5. Q: How secure is Wi-Fi Protected Access?

A: Wi-Fi Protected Access is a very strong wireless security enhancement. While no security solution can ever claim to be "absolutely secure", the protection that Wi-Fi Protected Access provides is significant. Many cryptographers are confident that Wi-Fi Protected Access addresses all the known attacks on WEP. It also adds strong user authentication, which was absent in WEP.

6. Q: Will products that support Wi-Fi Protected Access ship with it turned on or off as the default?

A: Initially, the Wi-Fi Alliance will allow vendors the option to ship with Wi-Fi Protected Access turned on or off. Eventually, it may be a requirement to ship with it turned on.

7. Q: When will products with Wi-Fi Protected Access be available?

A: Initial shipments of products with Wi-Fi Protected Access are expected to begin in May 2003. Many other vendors will ship during the course of 2003.

8. Q: Will this work for home and SOHO users?

A: Yes. Wi-Fi Protected Access has a special mode designed for home and SOHO users who will not have access to network servers. In this mode, the home or SOHO user manually enters the starting password to activate Wi-Fi Protected Access.

9. Q: Will enterprise users be replacing their proprietary security solutions and will they be replacing them with Wi-Fi Protected Access?

A: Most enterprise customers have been seeking standards-based, interoperable, strong Wi-Fi security and have only adopted proprietary technologies because nothing like Wi-Fi Protected Access has been available. Once Wi-Fi Protected Access products are available, we initially expect some companies to deploy only Wi-Fi Protected Access, some companies to have a mix of Wi-Fi Protected Access and proprietary solutions, and some companies to continue to use their proprietary solutions. We expect rapid deployment of Wi-Fi Protected Access particularly in companies that utilize Wi-Fi products from several different vendors. Longer term, we expect the majority of companies to migrate to Wi-Fi Protected Access as a standards-based solution.

10. Q: When will the Wi-Fi Alliance start certifying Wi-Fi Protected Access products?

A: The Wi-Fi Alliance will start certifying Wi-Fi Protected Access in April 2003. Initially, it will be optional for obtaining Wi-Fi Certification, as the Wi-Fi Alliance will allow vendors a phase-in period. Before the end of 2003, Wi-Fi Protected Access will be a mandatory part of the Wi-Fi Certification process.

11. Q: Will Wi-Fi Protected Access security work with existing Wi-Fi CERTIFIED wireless LAN products?

A: Yes, assuming the existing products have already been upgraded for Wi-Fi Protected Access. As mentioned above, Wi-Fi Protected Access is designed to be a software upgrade.

12. Q: Will Wi-Fi Protected Access operate in a network that has both WEP and Wi-Fi Protected Access components?

A: The Wi-Fi Alliance does not test or support a "mixed mode" of both WEP and Wi-Fi client devices. However, in a large network with many clients, a likely scenario is that Access Points will be upgraded before all the Wi-Fi clients can be upgraded. Some Access Points may support a mixed mode, which supports both clients running Wi-Fi Protected Access and clients running original WEP security. The cost of supporting both modes is that security is effectively at the minimum level allowed by the Access Point (i.e., WEP), so organizations will benefit by accelerating the move to Wi-Fi Protected Access for all Wi-Fi stations, and setting their Access Points to allow only Wi-Fi Protected Access.

13. Q: What is involved in upgrading Access Points and clients to Wi-Fi Protected Access?

A: Access Points will require a software upgrade. Clients will require a software upgrade for the network interface card, and possibly a software update for the operating system. For enterprise networks, an authentication server, typically one that supports RADIUS and the selected EAP authentication protocol, will be added to the network.

Press and analyst contact:

Lisa Grantham

Edelman

650.429.2758

lisa.grantham@edelman.com

rev. 12/30/2004