Q&A

WPA2™

1. **Q: Is WPA2 based on IEEE standards?**

   A: Yes, WPA2 is based on the IEEE 802.11i standard.

2. **Q: What's the relationship between IEEE 802.11i and WPA2?**

   A: All products that are Wi-Fi CERTIFIED™ for WPA2 are based on the IEEE 802.11i standard and implement the mandatory elements of that standard. WPA2 is the approved Wi-Fi Alliance interoperable implementation of 802.11i.

3. **Q: When will the Wi-Fi Alliance begin performing interoperability certification testing on WPA2?**

   A: Certification testing is scheduled to begin on September 1st, 2004.

4. **Q: When will products that are Wi-Fi CERTIFIED for WPA2 be available?**

   A: September 2004. The Wi-Fi Alliance is announcing on September 1st the availability of the first set of products that have been Wi-Fi CERTIFIED for WPA2. Many additional products will become Wi-Fi CERTIFIED for WPA2 over the coming weeks and months.

5. **Q: How are WPA™ and WPA2 similar?**

   A: Both WPA and WPA2 offer a high level of assurance for end-users and network administrators that their data will remain private and access to their network restricted to authorized users.

   Both utilize 802.1X and Extensible Authentication Protocol (EAP) for authentication. Both have Personal and Enterprise modes of operation that meet the distinct needs of the two different consumer and enterprise market segments.

6. **Q: How are WPA and WPA2 different?**

   A: WPA2 provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some corporate and government users.

7. **Q: Is WPA2 backward compatible with WPA?**

   A: Yes. All products Wi-Fi CERTIFIED for WPA2 will be interoperable with products that are Wi-Fi CERTIFIED for WPA.

8. **Q: Can WPA products be upgraded to WPA2? If so, what is required?**

   A: Some WPA products may be able to be upgraded to WPA2 by software. Others may require a hardware change due to the computationally intensive nature of WPA2's required AES encryption.

9. **Q: Is WPA2 backwards compatible to WEP?**

   A: The Wi-Fi Alliance does not consider WEP to be a secure solution. For security reasons, like WPA, products running in WPA2 mode cannot support WEP devices at the same time.

   However, for legacy device compatibility, WEP remains part of the baseline interoperability test for all Wi-Fi CERTIFIED products. Over time, the Alliance may drop WEP as a requirement for Wi-Fi Certification.

10. **Q: Does WPA2 offer Personal and Enterprise versions?**

    A: Like WPA, WPA2 offers both a Personal and Enterprise mode of operation. In the Personal mode of operation, a pre-shared key (password) is used for authentication, while in the Enterprise mode of operation, authentication is achieved via 802.1X and the EAP. Personal mode requires only an access point and client device, while Enterprise mode typically requires a RADIUS or other authentication server on the network.

11. **Q: How does WPA2 provide authentication?**

    A: WPA2 - Enterprise provides authentication using IEEE 802.1X and EAP. WPA2 - Personal provides authentication via a pre-shared key, or password.

12. **Q: How does WPA2 provide data encryption?**

    A: WPA2 provides data encryption via the AES. In contrast, WPA uses Temporal Key Integrity Protocol (TKIP).

13. **Q: Does WPA2 have session keys?**

    A: Like WPA, WPA2 creates fresh session keys on every association. The benefit is that the encryption keys used for each client on the network are unique and specific to that client. Ultimately, every packet sent over the air is encrypted with a unique key. The ability to avoid key reuse and provide unique, fresh encryption keys is a basic tenet of good security practice and is why both WPA and WPA2 offer such good security.

14. **Q: Will enterprise adoption of Wi-Fi® networks increase after the release of WPA2?**

    A: An increase in deployments of Wi-Fi networks in government and business is expected to follow the release of products that are Wi-Fi CERTIFIED for WPA2.

15. **Q: Is WPA still secure?**

    A: Yes, WPA remains secure. WPA is the major upgrade to Wi-Fi security, applicable to enterprise and home users. WPA was independently verified to address all of WEP's known weaknesses. WPA2 is not being released to address any flaws in WPA.

16. **Q: Why is the Alliance introducing WPA2?**

    A: Some corporate users want Wi-Fi CERTIFIED products based on the full 802.11i standard. Some government agencies require a security solution that can meet the FIPS 140-2 requirement, which WPA2's AES addresses.

Press and analyst contact:

Lisa Grantham
Edelman
650.429.2758
lisa.grantham@edelman.com

rev. 3/23/2005