Wi-Fi CERTIFIED WPA3™

Technology Overview

December 2019

Next-generation Wi-Fi® security for personal and enterprise networks

The use and ubiquity of Wi-Fi® has shepherded in a new era of constant connectivity. People and organizations the world over depend upon Wi-Fi to stay connected to others, entertain themselves, and remain productive everywhere they go. The massive growth in Wi-Fi device types, from smart home appliances to personal health monitoring equipment, has brought unprecedented convenience and value, and has changed the landscape of Wi-Fi networks. As the industry grows, Wi-Fi Alliance® has been there to nurture that growth with solutions that help standardize the technology we use and bring a better Wi-Fi experience.

With Wi-Fi growth comes an ever-changing challenge: security. Since its inception, Wi-Fi Alliance has continually worked to provide Wi-Fi users with secure Wi-Fi connections to protect user data. The evolution of Wi-Fi security solutions brings user confidence that helps underpin the success of Wi-Fi today. In 2003, Wi-Fi Alliance introduced the Wi-Fi Protected Access® family of technologies to help users protect their data. Since 2006, every Wi-Fi device has shipped with WPA2™ security, and over time the program has been enhanced to keep up with the changing security landscape. Now a whole new generation of Wi-Fi devices are now shipping with the latest in security protections that Wi-Fi CERTIFIED WPA3™ provides. Since WPA3™ is required for Wi-Fi CERTIFIED 6™ devices, WPA3 security will soon be widely available worldwide.

Wi-Fi security for the next generation of connectivity should also provide enhanced data protections for security-sensitive segments, such as financial institutions, healthcare, and governments. These needs are addressed in the next evolution of the Wi-Fi Protected Access family, which provides protections specified for personal and enterprise settings.

Wi-Fi CERTIFIED WPA3

Wi-Fi CERTIFIED WPA3 delivers the capabilities necessary to meet the requirements of different network deployments—ranging from highly controlled corporate environments to more flexible home networks—and to operate in different device form factors. Regardless of the environment or device type, all WPA3 devices deliver two key benefits:

- **Cryptographic consistency**: WPA3 reduces the susceptibility of networks to a successful attack by mandating policies around the use of Advanced Encryption Standard (AES) with legacy protocols, such as Temporal Key Integrity Protocol (TKIP).
- **Network Resiliency**: Protected Management Frames (PMF) deliver a level of protection against eavesdropping and forging for robust management frames. The consistent use of these protections improves the resiliency of mission-critical networks.

Wi-Fi Alliance first introduced PMF as an optional feature of WPA2 in 2012 and later mandated the capability for all Wi-Fi CERTIFIED™ ac devices. With the release of WPA3, Wi-Fi Alliance now mandates the use of Protected Management Frames in all WPA3 modes, providing protection for unicast and multicast robust management frames to include Action, Disassociate, and Deauthenticate frames.

WPA3-Personal provides robust password-based authentication

WPA3-Personal replaces the Pre-Shared Key (PSK) used in WPA2-Personal with Simultaneous Authentication of Equals (SAE), delivering more robust password-based authentication. WPA3-Personal uses passwords for authentication by proving knowledge of the password and not for key derivation, providing users with stronger security protections such as:

- **Offline dictionary attack resistance**: It is not possible for an adversary to passively observe a WPA3-Personal exchange or actively engage in a single WPA3-Personal exchange and then try all possible passwords without further interaction with the network to determine the correct password. The only method for determining the network password is through repeated active attacks in which the adversary gets only one guess at the password per attack.

- **Key recovery resistance**: Even if an adversary determines the password, it is not possible to passively observe an exchange and determine the session keys, providing forward secrecy of network traffic.
- **Natural password use**: Onerous complexity requirements when choosing a password make it difficult to use and are an impediment to delivering desired security protections. Because WPA3-Personal is resistant to offline dictionary attacks, users can choose passwords that are easier to remember and easier to enter while still retaining a high level of security.
- **Simple work flow continuity**: WPA3-Personal retains the ease-of-use and system maintenance associated with previous versions of personal Wi-Fi security.

Simultaneous Authentication of Equals

WPA3-Personal is based on Simultaneous Authentication of Equals (SAE), defined in Institute of Electrical and Electronics Engineers (IEEE) Std 802.11-2016. The Wi-Fi Alliance WPA3 Specification defines additional requirements for devices operating in SAE modes. SAE is a key exchange protocol that authenticates two peers using only a password, resulting in a shared secret between the two peers that can be used for secret communication while exchanging data over a public network. It provides a secure alternative to using certificates or when a centralized authority is not available.

In a Wi-Fi infrastructure network, the SAE handshake negotiates a fresh Pairwise Master Key (PMK) per client, which is then used in a traditional Wi-Fi four-way handshake to generate session keys. Neither the PMK nor the password credential used in the SAE exchange can be obtained by a passive attack, active attack, or offline dictionary attack. Password recovery is only possible through repeated active attacks guessing a different password each time. Additionally, forward secrecy is provided because the SAE handshake assures the PMK cannot be recovered if the password becomes known.

Transitioning to a WPA3-Personal network

When users begin to adopt WPA3-Personal networks, they can leverage WPA3-Personal Transition Mode, defined as WPA3-SAE Transition Mode in the Wi-Fi Alliance WPA3 Specification. WPA3-Personal Transition Mode allows for gradual migration to a WPA3-Personal network while maintaining interoperability with WPA2-Personal devices and without disruption to users. As more client devices include WPA3-Personal, they will benefit from the new protections provided without noticing since there is no need for additional user configuration.

A WPA3-Personal access point (AP) in transition mode enables WPA2-Personal and WPA3-Personal simultaneously on a single basic service set (BSS) to support client devices using a mix of WPA2-Personal and WPA3-Personal with the same passphrase. Client devices that support both WPA2-Personal and WPA3-Personal connect using the higher-security method of WPA3-Personal when available. To ensure interoperability with legacy devices that do not support PMF, WPA3-Personal Transition Mode configures the network as PMF capable (Management Frame Protection Capable bit = 1 and Management Frame Protection Required bit = 0), rather than PMF required. All WPA3-Personal connections must negotiate PMF even when connecting to a BSS where WPA3-Transition Mode is enabled.

The full benefits of WPA3-Personal are only available when *not* operating in WPA3-Personal Transition Mode. Once WPA3-Personal availability reaches a sufficient level amongst client devices, network owners should disable WPA3-Personal Transition Mode.

WPA3-Personal delivers more consistent cryptography

One of the key benefits of WPA3 is improved consistency in the application of cryptography. WPA3-Personal Transition Mode provides backwards interoperability with WPA2-Personal; other legacy protocols are disallowed in this mode. For example, WPA3-Personal is never combined on the same BSS as TKIP, even when operating in WPA3-Personal Transition Mode.

Similarly, configuring a BSS for WPA3-Personal requires the use of PMF, while WPA3-Personal Transition Mode allows non-PMF-capable clients to connect. However, every device supporting WPA3-Personal supports PMF, and

they must always negotiate management frame protection. The network will reject association by any device not adhering to these policies.

WPA3-Enterprise

WPA3-Enterprise does not fundamentally change or replace the protocols defined in WPA2-Enterprise. Instead, WPA3-Enterprise defines and enforces policies to deliver greater consistency in the *application* of those protocols to ensure desired security. In enterprise deployments, there are often multiple components with numerous options needing configuration to perform successful authentication and protect network traffic. This complexity gives rise to situations where the combination of configured components does not meet the expected security of the resulting exchange.

WPA3-Enterprise server certificate validation

Some WPA3-Enterprise implementations rely on the end user to determine the validity of the Remote Authentication Dial-In User Service (RADIUS) server and infrastructure to which they are connecting. RADIUS servers can also be configured with self-signed certificates which the end user or client device may blindly trust. An adversary that obtains a man-in-the-middle position is able to read, intercept, and manipulate data sent over the network, and in some cases to observe the "inner" client authentication exchange and crack the username or password. Since these credentials may also be used for corporate IT access in some enterprise deployments, this represents a potentially severe privacy threat.

WPA3-Enterprise server certificate validation requires the client device to validate the RADIUS server certificate before accessing a network. Validating the correct RADIUS server in a WPA3-Enterprise network can help prevent man-in-the-middle attacks. This feature also defines a Transport Layer Security (TLS) certificate policy to provide network administrators with tools to prevent users from inadvertently accepting server certificates of unknown networks.

Transitioning to a WPA3-Enterprise network

There is no need for a WPA3-Enterprise transition mode because WPA3-Enterprise does not fundamentally change or replace the protocols defined in WPA2-Enterprise. WPA2-Enterprise client devices will continue to interoperate with WPA3-Enterprise networks. A key consideration for network administrators is when to require PMF for all client device connections. While Wi-Fi Alliance has mandated PMF support in all Wi-Fi CERTIFIED™ ac devices since 2014, some networks must support legacy clients devoid of PMF capabilities.

A WPA3-Enterprise AP may offer two PMF configuration options for a WPA3-Enterprise network: PMF capable (Management Frame Protection Capable bit = 1 and Management Frame Protection Required bit = 0) and PMF required (Management Frame Protection Capable bit = 1 and Management Frame Protection Required bit = 1). Disabling PMF for a WPA3-Enterprise network is not an option. When configured as PMF capable, WPA2-Enterprise client devices will negotiate PMF. WPA3-Enterprise clients devices must use PMF. This configuration delivers interoperability with devices that do not support PMF. When configured as PMF required, WPA2-Enterprise and WPA3-Enterprise client devices must use PMF.

WPA3-Enterprise offers optional 192-bit security mode

For sensitive security environments, WPA3-Enterprise offers an optional 192-bit security mode that specifies the configuration of each cryptographic component such that the overall security of the network is consistent. This not only delivers the desired security level but also makes provisioning easier. The approach is based on the concept that cryptographic primitives have a work factor necessary for successful attack, and an attacker will target the weakest component in a system.

To achieve a consistent level of system security it is necessary to ensure that the work factor for each cryptographic primitive meets or exceeds a selected level. For example, it does no good to derive a 256-bit AES key from a shared secret resulting from a Diffie-Hellman group with a work factor of 2^{80}. Much like links in a chain, the overall security of the system is that of its weakest component.

The WPA3-Enterprise 192-bit security mode uses 256-bit Galois/Counter Mode Protocol (GCMP), widely written as GCMP-256, to provide authenticated encryption, 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384) for key derivation and key confirmation, and Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve for key establishment and authentication. While GCMP-192 would deliver the appropriate equivalent strength, GCMP-256 was selected based on its broader adoption. Misuse resistance is an important component of this new security mode, and Wi-Fi CERTIFIED devices do not allow configuration in a way that results in security less than the selected level.

By design, WPA3-Enterprise 192-bit security mode does not allow configuration in a way that would degrade security protections below the defined level. A network configured for 192-bit security requires all client devices to also operate in 192-bit security mode.

Fast BSS transition between secure networks

Many services on mobile devices are sensitive to roaming delays, particularly for voice and video traffic. Fast BSS transition provides a consistent user experience between secure networks for roaming between access points within a secure network. Fast BSS transition is available WPA3-Personal, WPA3-Personal transition mode, WPA3-Enterprise, WPA3-Enterprise Transition Mode, and can be used within an enterprise network, or within a home where multiple access points are deployed.

Usage examples for WPA3

Connected home

A wide variety of client devices are connected to home networks over Wi-Fi, including smartphones, tablets, laptops, set-top boxes, smart TVs, HDMI media sticks, smart speakers, home automation devices, and more.

Today, almost all Wi-Fi home networks are secured using WPA2-Personal with a Pre-Shared Key (PSK), which the user has chosen so that it is not easily guessable by someone trying to gain access to, or attack, the network.

When the user or service provider upgrades a home router to support WPA3-Personal, if WPA3-Personal Transition Mode on the AP is configured with the same passphrase as before all of the existing Wi-Fi devices will be able to connect to the new home router without any reconfiguration. When the user acquires new client devices that support WPA3-Personal, or certain existing client devices receive a software update that adds WPA3-Personal support, those client devices will automatically take advantage of the enhanced level of security provided by WPA3-Personal.

At such time when all user client devices support WPA3-Personal, the user or service provider can reconfigure the AP to operate in WPA3-Personal only mode (without WPA3-Personal Transition Mode support for WPA2-Personal devices) in order to obtain the maximum security benefits provided by WPA3-Personal. If the user has configured a separate guest network for visitors, WPA3-Personal Transition Mode can still be maintained on that segregated network so that guests, whose client devices might not yet support WPA3-Personal, can still connect without impacting the security level on the main home network.

Sensitive enterprise deployments

There are not many more data sensitive environments than a hospital. Hospitals not only contain very sensitive material in the form of patient records, but active device monitoring may be managed increasingly through next generation Wi-Fi networks. Those responsible for hospital data security and privacy continually update the hospital network policies around zero-day attacks and the latest security measures to protect all data in the network, including business critical applications and life critical medical devices running on Wi-Fi networks segmented by security policy. Implementing WPA3-Enterprise with 192-bit security will bring the hospital greater protection against future attacks and malware, while keeping up with the latest security methods. A WPA3 network builds upon the robust WPA2-Enterprise methods and provides for the secure transport of Wi-Fi traffic for thousands of connected devices.

Summary

The next generation of Wi-Fi connectivity requires robust tools and practices to maintain user data privacy and security. Wi-Fi Alliance has continued its track record of constantly evolving the Wi-Fi Protected Access family of technologies to provide the latest in security as the landscape changes. Through use of standards-based mechanisms, consistent application of protocols, and security interface tools that are easy to use, network owners can better protect user data and promote adoption of security best practices. That said, every network environment is different. Wi-Fi Alliance recognizes the need for robust solutions that meet the security requirements of a variety of device types and networks.

Through WPA3 and other programs such as Wi-Fi CERTIFIED Easy Connect™, Wi-Fi Alliance brings new capabilities that support the way the world works and lives today. Providing for secure onboarding of every type of device with greater simplicity and enabling user data protection for personal and data sensitive Wi-Fi network environments increase Wi-Fi user experience, as well as dependence on Wi-Fi.

WPA3 builds upon trusted WPA2 success to bring a new level of security for personal and enterprise environments with robust security protocols. Focus on cryptographic consistency, robust password-based authentication, and 192-bit security usher the market into the next age of connectivity with confidence.

More information about WPA3 is available at: https://www.wi-fi.org/discover-wi-fi/security.

About Wi-Fi Alliance®

www.wi-fi.org

Wi-Fi Alliance® is the worldwide network of companies that brings you Wi-Fi®. Members of our collaboration forum come together from across the Wi-Fi ecosystem with the shared vision to connect everyone and everything, everywhere, while providing the best possible user experience. Since 2000, Wi-Fi Alliance has completed more than 50,000 Wi-Fi certifications. The Wi-Fi CERTIFIED™ seal of approval designates products with proven interoperability, backward compatibility, and the highest industry-standard security protections in place. Today, Wi-Fi carries more than half of the internet's traffic in an ever-expanding variety of applications. Wi-Fi Alliance continues to drive the adoption and evolution of Wi-Fi, which billions of people rely on every day.