White Paper

Networking | Security
2021

Seamless Next-generation Wi-Fi Security Through Multivendor End-to-end WPA3 Verification

WPA3 is the latest generation of Wi-Fi security, bringing simplicity, backwards compatibility, and enhanced security. Intel Wi-Fi clients are certified and industry-tested—ready to equip your organization with higher network protection and minimal deployment effort.

Authors

Cosmin Cazan
Systems Engineer - Wireless Validation

Mohammad Y Mansour
Software Engineering Manager - Wireless

Table of Contents

Executive Summary

Wi-Fi Protected Access 3 (WPA3) is the latest improvement in Wi-Fi security, announced by the Wi-Fi Alliance® in 2018 as "Wi-Fi CERTIFIED WPA3™." It brings enhanced security protections for personal, enterprise, and even open Wi-Fi networks, mitigating vulnerabilities found in the preceding standard: WPA2[1].

Intel® Wi-Fi Adapters are WPA3-certified and have been thoroughly validated for interoperability and performance with major AP vendors, helping to ensure that both consumer and enterprise customers will have a smooth, more secure experience[2]. All supported WPA3 security modes and related components have been evaluated to alleviate concerns associated with moving to a new security standard. In addition, transition mode —which provides backwards compatibility for legacy WPA2-only clients — has also been verified, giving customers an intermediary option before fully committing to the adoption of WPA3.

Upgrading a personal, small-business, or enterprise network to WPA3 can be a simple process, with many existing devices and infrastructure supporting the latest standard. In some cases, devices will have a limited ability to roam from WPA3 to WPA2 networks to maintain elevated security, but this can be overcome as needed with network planning to accommodate for older devices. WPA3 provides the robust protocols that are worth upgrading to for a more secure wireless network.

Wi-Fi Security—Brief History

Wi-Fi has increasingly become a ubiquitous and essential part of our lives. Billions of devices around the world keep people connected, and Wi-Fi is used for critical tasks, from work and education to hospitals and government buildings. Maintaining highly secure Wi-Fi networks has been a goal and challenge since the early stages of Wi-Fi. Security standards have been evolving and improving, giving us a solid foundation for today's WPA3 standard. Figure 1 below illustrates the high-level Wi-Fi security release timeline.

The original Wired Equivalent Privacy (WEP) standard was ratified as a Wi-Fi security standard in 1999. It required 10-digit or 26-digit hexadecimal keys, making it difficult for regular users to remember the pre-shared key (PSK), while its serious cryptographic weaknesses made it easy to exploit. In 2003, a new standard called Wi-Fi Protected Access (WPA) emerged alongside the new 802.11g Wi-Fi standard. WPA introduced the concept of human-friendly Wi-Fi passwords and the Temporal Key Integrity Protocol (TKIP), a protocol designed to prevent replay attacks, which its predecessor, WEP, was highly susceptible to.

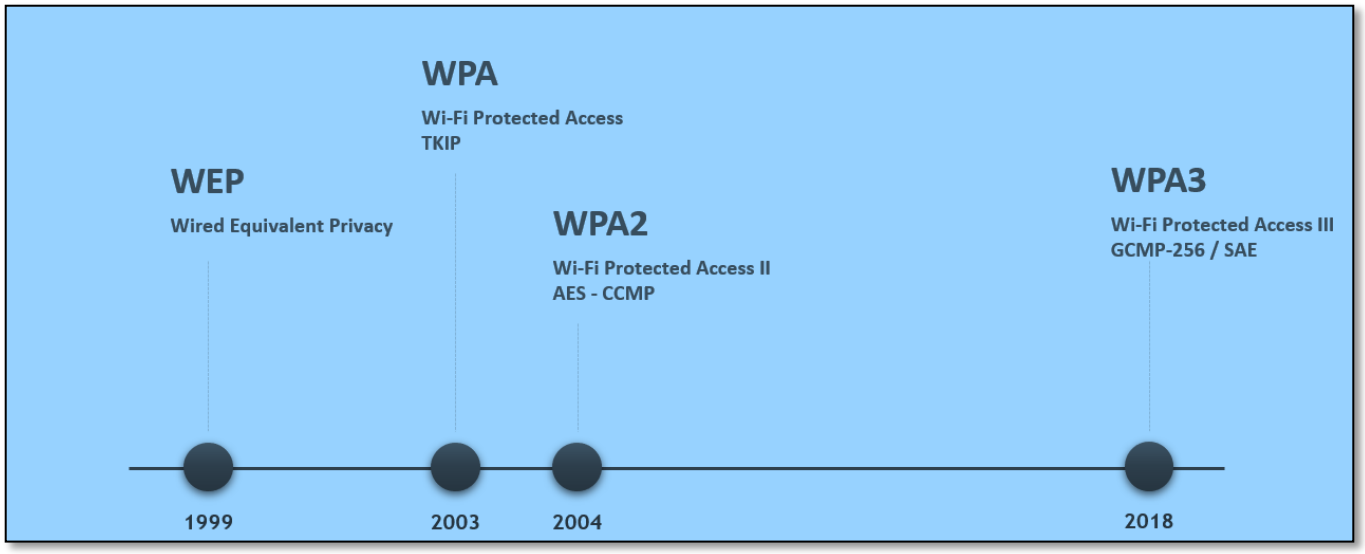

Figure 1. Wi-Fi Security Timeline

But WPA soon proved susceptible to other vulnerabilities, including man-in-the-middle attacks.

In 2004, the IEEE introduced the 802.11i addendum/security standard and with it, the Wi-Fi Alliance announced the WPA2 program for Wi-Fi product certification. This update added new encryption standards and ciphers, namely Advanced Encryption Standard (AES), and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). These new security standards proved robust over the next decade and more, with WPA2 still being the major Wi-Fi security standard in use today.

A later update to WPA2, in 2012, first introduced Protected Management Frames (PMF) as an optional feature. PMF capability was later made mandatory for Wi-Fi 5 devices, providing protection for management frames and paving the way for WPA3, which would continue its use of PMF and make its usage mandatory in all Wi-Fi networks, including personal.

Acronyms

WPA	Wi-Fi Protected Access
WEP	Wired Equivalent Privacy
TKIP	Temporal Key Integrity Protocol
PSK	Pre-Shared Key
SAE	Simultaneous Authentication of Equals
OWE	Opportunistic Wireless Encryption
AES	Advanced Encryption Standard
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
GCMP	Galois Counter Mode Protocol
PMF	Protected Management Frames
CNSA	Commercial National Security Algorithm

WPA3 Overview

WPA3 is the next-generation Wi-Fi security for personal and enterprise networks. It delivers key updates while maintaining backwards compatibility support for WPA2 clients with preexisting authentication and encryption types. In Figure 2, we've summarized the main differences between WPA2 and WPA3.

- WPA3 dictates use of robust standards such as AES and use of the latest security methods. It adds a 192-bit security mode, while eliminating use of legacy protocols such as TKIP
- WPA3 enforces mandatory PMF usage to improve network resiliency
- WPA3 provides a transition mode such that legacy WPA2 clients can still connect to most WPA3 networks

WPA3-Personal introduces a new more secure and more robust method of authentication for personal networks, replacing PSK: Simultaneous Authentication of Equals (SAE). This method is resistant to offline dictionary attacks and protects users, even when selecting short Wi-Fi passwords. In addition, it also protects data traffic even if a password is compromised at a later time with forward secrecy.

WPA3-Enterprise builds upon WPA2 by mandating use of PMF across networks, adding new encryption protocols such as Galois Counter Mode Protocol (GCMP), and even adding a 192-bit security mode that ensures the highest level of authentication and cryptography is used: Commercial National Security Algorithm Suite (CNSA), alternatively known as SuiteB.

On a parallel track, the Wi-Fi Alliance brought the use of PMF and higher security even to open Wi-Fi networks through its Wi-Fi CERTIFIED Enhanced Open™ program. Relying on Opportunistic Wireless Encryption (OWE), an Enhanced Open network provides unauthenticated data encryption, reducing some of the privacy risks associated with open networks.

Features	WPA2	WPA3
Encryption	AES-CCMP	GCMP-256 / AES-CCMP
Authentication	PSK / 802.1x with EAP	SAE / 802.1x with EAP
Key Length	128-bit	192-bit
Protected Management Frames *(PMF)*	Optional	Mandatory
Attack resiliency *KRACK, Offline Dictionary*		✓

Figure 2. WPA3 compared to WPA2

Supported Modes and Industry Verification

Intel® Wi-Fi Adapters are WPA3-certified and support all the major improvements brought on by WPA3 and Enhanced Open. In addition, all the supported WPA3 security modes and related components have been thoroughly verified for interoperability and performance with major Wi-Fi access point vendors.

In Figure 3, we've created a simplified, but clear, matrix to showcase the WPA3 modes and combinations that are supported and verified.

- WPA3-Personal/SAE is the new standard for personal Wi-Fi security. It's most secure when used exclusively for a personal SSID, but it can coexist with WPA2 PSK authentication, offering a backwards-compatible avenue for legacy WPA2 clients that don't have the required support for SAE. This newly added method of authentication, using a dragonfly key exchange, makes it resilient to offline dictionary attacks and provides forward secrecy. Due to the multilayer generation of keys, even if an attacker were to guess the password at a later time, they wouldn't be able to decrypt the users' data. SAE is the only authentication method for personal security supported in Wi-Fi 6E.
- OWE/Enhanced Open is the new standard for open Wi-Fi networks, providing some security even without authentication and eliminating text in the clear. It supports transition mode, allowing legacy clients to connect to a legacy open network. Wi-Fi 6E eliminates the use of legacy open networks, with the goal of ensuring that all Wi-Fi sessions have at least a minimum level of privacy and protection.
- WPA3-Enterprise/AES-CCMP 802.1x builds on current WPA2 enterprise protocols but dictates the use of PMF for WPA3 clients to increase network resiliency. It allows backwards compatibility by advertising PMF-capable networks in transition mode, rather than PMF-required networks in WPA3-only mode. This would ensure that legacy WPA2 clients can connect as well.
- WPA3-Enterprise/GCMP-256 192-bit with Secure Hash Algorithm (HMAC-SHA384) is a new, highly secure mode for security-sensitive environments. By design this mode doesn't allow a transition mode to maintain the high level of security it was intended for. Therefore, this mode is only available for WPA3 clients, with no backwards compatibility for legacy WPA2 clients.

It's important to note that the recently ratified Wi-Fi 6E standard mandates the use of WPA3 security. As such, the motivation and benefit to upgrade Wi-Fi networks to WPA3 now is very palpable.

All the modes described in this white paper have been verified for interoperability and performance with major Wi-Fi access point vendors by Intel and other industry partners, using Intel Wi-Fi Adapters and current-generation access points from major vendors, giving customers a high level of confidence that their organizations can smoothly migrate to WPA3.

Figure 3. WPA3 Modes Supported by Intel Wi-Fi Adapters

WPA3 Security Mode	Transition Mode (Backwards Compatible with WPA2 clients)	Traditional Wi-Fi Bands 2.4 & 5 GHz	Wi-Fi 6E 6 GHz	Windows	Linux
WPA3 – SAE *(Personal)*	✓	✓	✓	✓	✓
WPA3 – OWE *(Enhanced Open)*	✓	✓	✓	✓	✓
WPA3 – AES-CCMP *(Enterprise / 802.1x)*	✓	✓	✓	✓	✓
WPA3 – GCMP-256 *(Enterprise / 192-bit security)*		✓	✓	✓	✓

WPA3 Challenges

WPA3 brings concrete improvements to Wi-Fi security, making Wi-Fi networks universally more robust and more secure. History shows that adoption and deployment of new security standards is often slow. Intel, in collaboration with industry partners, has verified and shown that WPA3 is ready for deployment, but there are some limitations that operators need to be aware of.

Fast Transition (FT) is a widely used feature, as part of IEEE 802.11r standard, that minimizes roam time between access points. Intel Wi-Fi Adapter roaming with FT, on Windows OS, is currently only supported for WPA3 AES-CCMP 802.1x mode; it isn't supported with WPA3-Personal, WPA-3 Enterprise GCMP-128, nor WPA3-Enterprise 192-bit security modes. Figure 4 illustrates the FT support matrix.

WPA3 Security Mode	Windows Fast Transition (802.11r)	Linux Fast Transition (802.11r)
WPA3 – SAE *(Personal)*		✓
WPA3 – AES-CCMP *(Enterprise / 802.1x)*	✓	✓
WPA3 – GCMP-256 *(Enterprise / 192-bit security)*		✓

Figure 4. WPA3 Modes with Fast Transition[3]

In addition to FT, regular Wi-Fi roaming from WPA3 to WPA2 networks is also not generally supported by design to maintain security integrity. In certain deployments with mixed WPA3/WPA2 infrastructure and AP deployment, this may pose a challenge. The operator needs to ensure that WPA3 users can seamlessly roam across the network, without gaps in WPA3 support.

Conclusion

WPA3 is the latest and most secure option for Wi-Fi security. It has been improved to be simpler to use and more robust than ever. The new standard creates a higher level of protection and privacy for personal, enterprise and even open networks. Personal Wi-Fi networks using WPA3 are more resilient to classic replay and offline dictionary attacks; enterprise networks are more resilient with mandatory use of PMF and higher-bit security when the utmost level of security is needed; Enhanced Open networks have added privacy even without authentication, replacing text-in-the-clear data.

Intel Wi-Fi Adapters are WPA3-certified and have been thoroughly validated for interoperability and performance with major AP vendors, ensuring that both consumer and enterprise customers have a smooth and more secure Wi-Fi experience. All supported WPA3 security modes and related components have been evaluated with a wide range of access points to mitigate concerns associated with moving to a new security standard. In addition, transition mode—which provides backwards compatibility for legacy WPA2-only clients—has also been verified, giving customers the flexibility to evaluate the latest security standard without compromising connectivity for older devices.

1 Wi-Fi Alliance WPA3 Announcement — https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

2 For details on Intel Wi-Fi Adapters WPA3 support, visit https://www.intel.com/content/www/us/en/support/articles/000054783/network-and-i-o/wireless.html

3 Intel Wi-Fi adapters have been tested with latest Windows 10 OS build 19043 (2.4 and 5 GHz bands), on Windows 11 Insider Preview build 22000 (Wi-Fi 6E), and on Ubuntu 18.04