Wireless Broadband Alliance Issues New Wi-Fi Security Guidelines to Advance Trust, Privacy and Seamless Global Roaming

New guidelines provide a framework to lower operational risk and support seamless roaming at scale across public, enterprise and IoT environments

Logo of the Wireless Broadband Alliance

LONDON, UNITED KINGDOM, April 14, 2026 /EINPresswire.com/ -- The Wireless Broadband Alliance (WBA), the global industry body dedicated to driving the seamless and interoperable service experience of Wi-Fi across the global wireless ecosystem, today released a new Wi-Fi Security Guidelines report. The guidelines define a new industry framework designed to strengthen security, privacy and trust across Wi-Fi networks, including public, enterprise, IoT and roaming environments.

> These guidelines show how proven standards and best practices can be applied consistently to deliver secure, privacy-preserving, and interoperable Wi-Fi experiences."
>
> *Tiago Rodrigues, President and CEO, Wireless Broadband Alliance*

Today, Wi-Fi underpins critical digital services for consumers, businesses and connected devices, yet inconsistent or fragmented security practices can expose users and operators to risks ranging from rogue access points and credential theft, to privacy breaches and signaling attacks. The new guidelines will help organizations reduce exposure to common Wi-Fi threats, improve user trust, and simplify interoperability across networks and partners. For operators and enterprises, this results in more predictable security outcomes and greater confidence when deploying or scaling Wi-Fi services.

The guidelines address the growing need for carrier-grade security that aligns with user expectations. Built on widely deployed technologies including OpenRoaming™ and Passpoint®, the report sets out a clear, standards-based framework for securing Wi-Fi end-to-end, from device authentication through to physical and backhaul security, Layer-2 protection, RadSec adoption, federation governance and readiness for post-quantum cryptography.

Interoperable connectivity comparable to cellular networks

Implemented together, interoperable measures across authentication, encryption, identity privacy, credential handling, infrastructure, control-plane signaling and federation governance, enable Wi-Fi to deliver secure, privacy-preserving and interoperable connectivity comparable to cellular networks.

Tiago Rodrigues, President and CEO of the Wireless Broadband Alliance

The guidelines on securing Wi-Fi networks are designed to:

• Prevent connections to rogue and fake networks: Wi-Fi security starts with trust. The report mandates mutual authentication using 802.1X and strong EAP methods, requiring devices to validate network certificates before sharing credentials. This ensures users only connect to legitimate networks and significantly reduces the risk of evil-twin and rogue AP attacks

• Protect data over the air: By enforcing WPA2/WPA3-Enterprise with AES encryption and Protected Management Frames (PMF), the report ensures traffic confidentiality and integrity. This prevents passive sniffing, deauthentication attacks, and many man-in-the-middle techniques, bringing Wi-Fi security closer to cellular-grade protection

• Preserve user identity privacy without breaking compliance: The report balances privacy and traceability by using anonymous identities, encrypted inner identities, pseudonyms, and Chargeable-User-Identity (CUI). This protects personally identifiable information during authentication while still enabling lawful intercept, billing, and incident handling when required

• Secure credentials end-to-end: Credentials are protected throughout their lifecycle, from device to network to backend systems. The report requires secure OS key stores on devices, hardened credential storage in identity provider systems, and tamper-resistant SIM and USIMs for mobile credentials, reducing the risk of large-scale credential theft

• Harden the entire access network: Security extends beyond the radio link. The report provides guidance for physical security of access points and controllers, encrypted AP-to-controller links, secure backhaul design, and local breakout architectures, ensuring traffic remains protected across the full network path

• Secure AAA and roaming signaling: Recognizing that the control plane is often overlooked, the report strongly recommends RADIUS over TLS or DTLS for all AAA and roaming exchanges. This

protects authentication and accounting traffic from interception or manipulation, aligning with OpenRoaming and WRIX requirements

• Add Layer-2 protections against lateral attacks: To limit damage even if a malicious device connects, the report promotes Layer-2 traffic inspection, client isolation, proxy ARP, and multicast and broadcast controls, reducing client-to-client attacks such as ARP spoofing and broadcast abuse

• Enforce security through federation and governance: Security is reinforced not only technically but operationally. Through OpenRoaming and the WRIX legal framework, security requirements, responsibilities, and privacy obligations are consistently enforced across operators, identity providers, and hubs

The WBA has also created a Wi-Fi Security FAQ alongside the new guidelines. It gives users, enterprises and network operators a clear and accessible understanding of how modern Wi-Fi security works and can be seen at: https://wballiance.com/wi-fi-security-general-audience-faq

Tiago Rodrigues, President and CEO of the Wireless Broadband Alliance, said: “Today, Wi-Fi underpins critical connectivity for consumers, enterprises and IoT at global scale. These guidelines show how proven standards and best practices can be applied consistently to deliver secure, privacy-preserving, and interoperable Wi-Fi experiences. By aligning security across devices and networks, Wi-Fi achieves parity with cellular in security capability and confidence.”

Cameron Dunn, Assistant Vice President, In-Building Solutions, AT&T Services, Inc., adds: "For operators, secure Wi-Fi is essential to delivering trusted and seamless connectivity at scale. What this work shows is that, by applying established best practices across authentication, encryption, identity privacy, signaling and federation governance, Wi-Fi can provide the level of security and consistency needed for modern roaming and offload use cases.”

Nick Hudson, COO for UK and Ireland at Boldyn Networks, said: “At Boldyn Networks, we design and deploy advanced connectivity infrastructure for customers in many sectors who rely on our ability to provide secure and protected networks. We applaud WBA’s initiative to provide new Wi-Fi security guidelines and work together to continue shaping the industry standards”

Phil Morgan, CTO at NC-Expert, adds: “As wireless technology continues to underpin modern enterprise communication, we believe its security must be approached with precision, shared accountability, and oversight. These guidelines reflect our collective obligation to raise the standard of responsibility and governance.”

The Wi-Fi Security Guidelines report is available to download at https://wballiance.com/wba-wi-fi-security-guidelines/

About the Wireless Broadband Alliance

Wireless Broadband Alliance (WBA) is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the WBA is to drive seamless, interoperable Wi-Fi service experiences within the global wireless ecosystem. The WBA's mission is to bring together global industry leaders, collaborating to accelerate the development, integration and adoption of next-generation Wi-Fi and wireless technologies to deliver business growth, through innovation, technical and standards development, and real-world deployment programs.

Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, 6G, IoT, Smart Cities, Testing & Interoperability and Policy & Regulatory Affairs.

Membership in the WBA includes major operators, service providers, enterprises, hardware and software vendors, and other prominent companies that support the ecosystems from around the world. The WBA Board comprises influential organizations such as Airties, AT&T, Boingo Wireless, Boldyn Networks, BT, Charter Communications, Cisco Systems, Comcast, HFCL, HPE, Intel, Reliance Jio, RUCKUS Networks, Telecom Deutschland and Turk Telekom.

Wireless Broadband Alliance PR team
GingerPR Ltd
+44 1932 485300
email us here
Visit us on social media:
LinkedIn
Facebook
X