Wireless Broadband Alliance and FIDO Alliance Validate Secure, Zero-Touch Wi-Fi Onboarding for IoT and Edge Devices

Trial demonstrates factory-provisioned devices can connect automatically to OpenRoaming® and begin secure FIDO Device Onboard ownership transfer, cutting deployment costs



Logo of the Wireless Broadband Alliance

LONDON, UNITED KINGDOM, September 22, 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 announced the publication of the OpenRoaming® For IoT Trials Report, developed in collaboration with the FIDO Alliance. The report demonstrates that a standards-based approach can address persistent challenges in large IoT deployments for manufacturers and enterprises, reducing the cost and complexity of deploying connected devices at scale.

> “This work marks an important step, extending OpenRoaming further into IoT and edge device use cases...”
>
> *Tiago Rodrigues, President and CEO of the Wireless Broadband Alliance*

Securely bringing hundreds or thousands of devices online can require significant manual intervention, particularly when equipment is installed across multiple locations, networks and administrative domains. By combining OpenRoaming, Passpoint® and FIDO Device Onboard (FDO), IoT and edge devices can establish secure connectivity at first power-on, begin ownership transfer and receive the credentials and configuration required for their operational environment, without technicians manually configuring each device.

Testing results from the trials report

The new report details how the approach tested by WBA and the FIDO Alliance creates a repeatable onboarding model that reduces credential handling and deployment complexity, while maintaining enterprise control over where devices ultimately connect.

Key achievements recorded in the trials included:

- Zero-touch IoT onboarding is technically feasible. A factory-based credentials mechanism can be used to enable a device to connect automatically to an OpenRoaming network without manual Wi-Fi configuration
- OpenRoaming helps provide the secure bootstrap connection. It gives the device trusted initial connectivity before it transitions to its final enterprise, industrial or private network
- FDO helps manage secure ownership transfer and configuration. FIDO Device Onboard supports device identity, ownership transfer and delivery of network credentials, policies and application configuration
- Manufacturing becomes part of the trust framework. Device-bound certificates and credentials can be securely provisioned before shipment
- The model supports device redeployment. Devices can be reassigned and securely onboarded into new operational environments


Tiago Rodrigues, President and CEO of the Wireless Broadband Alliance

How the model works

Under the model, manufacturers can provision devices with cryptographically bound credentials before shipment. When powered up within range of an OpenRoaming-enabled network, the device then authenticates automatically and uses that initial connection to reach its onboarding services.

OpenRoaming acts as a secure bootstrap layer rather than dictating the device's final network placement. FDO manages device identity, ownership transfer and the delivery of operational credentials, policies and configuration. The device can then leave the bootstrap connection and move onto its designated enterprise, industrial, private or other operational network. This separation between initial access and final network placement enables organizations to automate onboarding without giving up control over local security policies and network access.

The trial team also described how this model could simplify the redeployment of connected products. Devices reassigned to a different site or owner can be securely re-onboarded into a new operational environment rather than requiring extensive manual reconfiguration.

A deeper look at the trial

The proof of concept was implemented by VinCSS using a Linux-based Raspberry Pi as a representative onboarding device and was designed to validate the first phase "End-user and

Device Onboarding Flow". Private keys were stored in a secure hardware element and were never exported. At first power-on, the device connected automatically to an available OpenRoaming network and initiated the FDO TO1 and TO2 ownership-transfer workflow. The trial successfully validated the initial FDO provisioning stage of the WBA OpenRoaming for IoT Model.

The report also identifies environments that require further technical work including air-gapped or high-security networks, restricted network segments and resource-constrained IoT devices that cannot run FDO or a Passpoint supplicant directly. For resource-constrained devices, the report explores a potential proxy model through which a helper device could execute the OpenRoaming and FDO protocols on their behalf. Solutions for air gapped applications are already in definition and are expected to be part of a future WBA-FDO applications report.

An invitation to industry
The WBA and FIDO Alliance are inviting device manufacturers, enterprises, operators, infrastructure providers and IoT solution developers to participate in the next phase of the work. Priorities include real-world, multi-vendor trials, industry-specific proofs of concept, certificate lifecycle testing and further development for air-gapped and resource-constrained environments.

Tiago Rodrigues, President and CEO of the Wireless Broadband Alliance, said: "This work marks an important step, extending OpenRoaming further into IoT and edge device use cases. By combining OpenRoaming's secure, interoperable connectivity with FIDO Device Onboard, we have shown how devices can establish a trusted first connection, begin automated onboarding and then transition to their designated operational network. It demonstrates the value of collaboration across the Wi-Fi, identity, manufacturing and IoT ecosystems, while providing a standards-based foundation for further interoperability testing, product development and real-world trials that can help reduce deployment overhead and strengthen device security at scale."

For more information on the trials including explanations of the model and areas for future work, download the OpenRoaming for IoT Trials Report at https://wballiance.com/openroaming-for-iot-device-onboarding

Mark Grayson, Cisco Fellow at Cisco, added: "Setting up large numbers of connected devices manually is a major hurdle for businesses today. This work empowers the manufacturing and enterprise industries to automatically connect and secure devices right out of the box, helping companies grow their networks more simply and securely."

Richard Kerslake, Market Development, Connected Standards at FIDO Alliance, said: "Enterprises no longer have to choose between speed and security. By pairing FIDO Device Onboard with OpenRoaming, devices can now authenticate, locate their network, and configure themselves automatically - with zero manual setup and zero risk of tampering. It's the secure, friction-free

blueprint that IoT and Edge applications need to scale in the real world."

Dr. Necati Canpolat, Sr. Staff, Next Generation and Standards, Intel, said: “As IoT deployments continue to scale, the industry needs a simpler and more secure way to bring devices online from first power-on. By combining trusted device identity established during manufacturing with OpenRoaming® and FIDO Device Onboard, this work demonstrates a practical path towards automated onboarding across diverse network environments. It is an important step towards making secure, zero-touch deployment easier to implement at scale.”

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 services 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, 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

This press release can be viewed online at: https://www.einpresswire.com/article/943995961

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.