IEEE P802.11
Wireless LANs

|  |
| --- |
| 802.11 Post Quantum Cryptography Proposed PAR |
| Date: 2025-05-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Juan-Carlos Zuniga | Cisco Systems |  |  | juzuniga@cisco.com |
| Stephen Orr | Cisco Systems |  |  | sorr@cisco.com |
| Dorothy Stanley | HPE |  |  | dorothy.stanley@hpe.com |
| Dan Harkins | HPE |  |  | Daniel.harkins@hpe.com |
| Stephen McCann | Huawei  |  |  | stephen.mccann@ieee.org |
| Michael Montemurro | Huawei |  |  | Montemurro.michael@gmail.com |
| Alexandru Lungu | Samsung |  |  | da.lungu@samsung.com |
| Mark Rison | Samsung |  |  | m.rison@samsung.com |
| Jay Yang | ZTE |  |  | yang.zhijie@zte.com.cn |

Abstract

This document contains the draft Project Authorization Request document for a new project, Enhancements for Post-Quantum Cryptography.

# PAR

**P802.11**

**Type of Project:** Amendment to IEEE Standard 802.11-2024
Project Request Type: Initiation/Amendment
**PAR Request Date:** TBD
**PAR Approval Date: [Populated after PAR approval]
PAR Expiration Date: [Populated after PAR approval]
PAR Status:** Draft
**Root Project**: 802.11-2024
**1.1 Project Number:** P802.11xx
**1.2 Type of Document:** Standard
**1.3 Life Cycle:** Full Use

**2.1 Title:** Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications--Amendment: Enhancements for Post-Quantum Cryptography

**3.1 Working Group:** Wireless LAN Working Group (C/LAN/MAN/802.11 WG)

**3.1.1Contact Information for Working Group Chair**

**Name: Robert Stacey**

**Email Address:** robert.stacey@intel.com
**Phone:** +1-503-724-0893

**3.1.2Contact Information for Working Group Vice-Chair**

**Name:** Jon Rosdahl
**Email Address:** jrosdahl@ieee.org
**Phone:** 801-492-4023

**3.2 Society and Committee:** IEEE Computer Society/LAN/MAN Standards Committee (C/LAN/MAN)

**3.2.1 Contact Information for Standards Committee Chair:
Name:** James Gilb **Email Address:** gilb\_ieee@tuta.com  **3.2.2 Contact Information for Standards Committee Vice Chair:
Name:** David Halasz **Email Address:** dave.halasz@ieee.org  **3.2.3 Contact Information for Standards Representative:
Name:** George Zimmerman **Email Address:** george@cmephyconsulting.com

**4.1 Type of Ballot:** Individual
**4.2 Expected Date of submission of draft to the IEEE-SA for Initial Standards Committee Ballot:** March 2027 **4.3 Projected Completion Date for Submittal to RevCom:** January 2028

**5.1 Approximate number of people expected to be actively involved in the development of this project:** 30

**5.2.a. Scope of the complete standard:** The scope of this standard is to define one medium access control (MAC) and several physical layer (PHY) specifications for wireless connectivity for fixed, portable, and moving stations (STAs) within a local area.

**5.2.b. Scope of the project:** This amendment extends 802.11 security to support algorithms for post-quantum cryptography (PQC). The extension specifies:

1. authentication and key management (AKM) suites for PQC,
2. digital signature and key establishment algorithms that use PQC,
3. a password authenticated key exchange that uses PQC,
4. modifications to key handshake protocols for PQC, and
5. addition of quantum resistant cipher suites and integrity protocols.

 **5.3 Is the completion of this standard dependent upon the completion of another standard:** No

**5.4 Purpose:** The purpose of this standard is to provide wireless connectivity for fixed, portable, and moving stations within a local area. This standard also offers regulatory bodies a means of standardizing access to one or more frequency bands for the purpose of local area communication.

**5.5 Need for the Project:** Classic public key cryptography, for example key exchanges based on Diffie-Hellman (both finite field and elliptic curve) and digital signatures based on the RSA cryptosystem, is vulnerable to compromise from a quantum computer adversary. There is a strong market need to define post-quantum protocols that support algorithms that are resistant to attacks by quantum computers (a.k.a. quantum-resistant) in the standard to address this anticipated vulnerability. As an example, the United States National Institute of Science and Technology (NIST) will disallow use of key establishment and digital signatures based classic cryptography for use in US government systems after 2035. NIST has published new post-quantum algorithms for use in key establishment and digital signature protocols. It is believed that these requirements will appear in other market verticals.

**5.6 Stakeholders for the Standard:**Manufacturers and users of semiconductors, personal computers, enterprise networking devices, consumer electronic devices, home networking equipment, mobile devices, and cellular operators.

**Intellectual Property:
6.1.a. Is the Standards Committee aware of any copyright permissions needed for this project?:** No
**6.1.b. Is the Standards Committee aware of possible registration activity related to this project?:** No

**7.1Are there other standards or projects with a similar scope?:** No

* 1. **Joint Development: Is it the intent to develop this document jointly with another organization?:** No

**8.1 Additional Explanatory Notes (Item Number and Explanation):**
5.5: The algorithms published by NIST are
FIPS 203, [Module-Lattice-Based Key-Encapsulation Mechanism Standard](https://csrc.nist.gov/pubs/fips/203/final)
FIPS 204, [Module-Lattice-Based Digital Signature Standard](https://csrc.nist.gov/pubs/fips/204/final), and
FIPS 205, [Stateless Hash-Based Digital Signature Standard](https://csrc.nist.gov/pubs/fips/205/final).

**References:**