IEEE SA STANDARDS ASSOCIATION

IEEE

P802.11bt

Type of Project: Amendment to IEEE Standard 802.11-2024
Project Request Type: Initiation / Amendment
PAR Request Date:
PAR Approval Date:
PAR Expiration Date:
PAR Status: Draft
Root Project: 802.11-2024

1.1 Project Number: P802.11bt
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Project Title: IEEE 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)
3.1.1 Contact Information for Working Group Chair:
Name: Robert Stacey
Email Address: rjstacey@gmail.com
3.1.2 Contact Information for Working Group Vice Chair:
Name: Jon Rosdahl
Email Address: jrosdahl@ieee.org
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: Mar 2027
4.3 Projected Completion Date for Submittal to RevCom: Jan 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:
a) Authentication and key management (AKM) suites for PQC,
b) Digital signature and key establishment algorithms that use PQC,
c) A password authenticated key exchange that uses PQC, and
d) Modifications to key handshake protocols for PQC.

5.3 Is the completion of this standard contingent 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 also 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.

6.1 Intellectual Property

6.1.1 Is the Standards Committee aware of any copyright permissions needed for this project? No

6.1.2 Is the Standards Committee aware of possible registration activity related to this project? No

---

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

7.2 Is it the intent to develop this document jointly with another organization? No

---

8.1 Additional Explanatory Notes: The algorithms published by NIST are
FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard
FIPS 204, Module-Lattice-Based Digital Signature Standard, and
FIPS 205, Stateless Hash-Based Digital Signature Standard.