IEEE P802.11
Wireless LANs

|  |
| --- |
| A CSD Proposal for Post-Quantum Cryptography (PQC) |
| Date: 2025-03-12 |
| 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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

CSD proposal for IEEE 802.11 Post-Quantum Cryptography Security Enhancements.

# 1. IEEE 802 criteria for standards development (CSD)

The CSD documents an agreement between the Working Group and the IEEE 802 LMSC that provides a description of the project and the IEEE 802 LMSC's requirements more detailed than required in the PAR. The CSD consists of the project process requirements, 14.1, and the 5C requirements, 14.2.

## 1.1 Project process requirements

### 1.1.1 Managed objects

Describe the plan for developing a definition of managed objects. The plan shall specify one of the following:

1. The definitions will be part of this project. **YES**
2. The definitions will be part of a different project and provide the plan for that project or anticipated future project.
3. The definitions will not be developed and explain why such definitions are not needed.

### 1.1.2 Coexistence

A WG proposing a wireless project shall demonstrate coexistence through the preparation of a Coexistence Assurance (CA) document unless it is not applicable.

1. Will the WG create a CA document as part of the WG balloting process as described in Clause 13? **NO**
2. If not, explain why the CA document is not applicable. **This project impacts MAC security operation only.**

##

## 1.2 5C requirements

## 1.2.1 Broad Market Potential

Each proposed IEEE 802 LMSC standard shall have broad market potential. At a minimum, address the following areas:

a) Broad sets of applicability.

 As of 2024, approximately 5.5 billion people worldwide are connected to the internet, which accounts for 68% of the global population [1], and majority of the traffic comes over WLAN [2]. WLAN continues to play a pivotal role in managing this surge in internet traffic and connecting billions of devices to the internet. The evolution of WLAN technology promises to deliver higher speeds, wider bandwidths, and lower latencies [3].

Cryptographically relevant post quantum computers are anticipated with some probability in the coming years. Accordingly certain responsible government authorities have defined procurement roadmaps for adoption of quantum resistant technologies, and the USA entity has recently advanced its timeline to 2027 [4].

Beyond the government market, due to the fact that a cryptographically relevant post quantum computer will void the security mechanisms used by all current IEEE 802.11 devices, the market segment for a post-quantum project are all uses of IEEE 802.11 that employ security.

b) Multiple vendors and numerous users.

 A wide variety of vendors currently build numerous products for the Wireless Local Area Network (WLAN) marketplace. It is anticipated that most of those vendors, and others, will participate in the standards development process and subsequent commercialization activities.

## 1.2.2 Compatibility

Each proposed IEEE 802 LMSC standard should be in conformance with IEEE Std 802, IEEE 802.1AC, and IEEE 802.1Q. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with IEEE 802.1 Working Group prior to submitting a PAR to the IEEE 802 LMSC.

1. Will the proposed standard comply with IEEE Std 802, IEEE Std 802.1AC and IEEE Std 802.1Q? **YES**
2. If the answer to a) is no, supply the response from the IEEE 802.1 WG.

The review and response is not required if the proposed standard is an amendment or revision to an existing standard for which it has been previously determined that compliance with the above IEEE 802 standards is not possible. In this case, the CSD statement shall state that this is the case.

## 1.2.3 Distinct Identity

Each proposed IEEE 802 LMSC standard shall provide evidence of a distinct identity. Identify standards and standards projects with similar scopes and for each one describe why the proposed project is substantially different.

------

 The proposed project focuses on employing newly approved algorithms that provide security in the presence of a cryptographically relevant quantum computer to support secure 802.11 communication. This includes both key establishment and authentication protocols.

There is no other WLAN project that is currently focused on post-quantum cryptography.

## 1.2.4 Technical Feasibility

Each proposed IEEE 802 LMSC standard shall provide evidence that the project is technically feasible within the time frame of the project. At a minimum, address the following items to demonstrate technical feasibility:

a) Demonstrated system feasibility.

 Algorithms for key exchange and digital signatures that provide security in the presence of a quantum computer have been analyzed and approved by cryptographers around the world. The proposed project will offer an upgrade to the classic cryptography algorithms in the IEEE 802.11 standard via these new post-quantum secure algorithms.

b) Proven similar technology via testing, modelling, simulation, etc.

(TBD)

**1.2.5 Economic Feasibility**

Each proposed IEEE 802 LMSC standard shall provide evidence of economic feasibility. Demonstrate, as far as can reasonably be estimated, the economic feasibility of the proposed project for its intended applications. Among the areas that may be addressed in the cost for performance analysis are the following:

a) Balanced costs (infrastructure versus attached stations).

 WLAN equipment is accepted as having balanced costs. Use of quantum-secure cryptographic algorithms will not alter this balance.

1. b) Known cost factors.

 Support of the proposed amendment will likely require manufacturers to develop modified firmware. This is a minor development cost. ..Several quantum-secure algorithms have large outputs which will not fit in a single MSDU, compelling fragmentation of frames. This fragmentation/reassembly will result in a cost being borne by both the transmitter and receiver, basically every WLAN device.

c) Consideration of installation costs.

 There are no anticipated installation costs with this project, beyond the negligible costs related to performing (remote) software upgrades.

d) Consideration of operational costs (e.g., energy consumption).

 A source of cryptographically strong entropy is needed by quantum-secure algorithms. This will introduce a minor increase operational cost versus existing classic cryptographic algorithms. This cost will be incurred only during initial handshaking and is amortized over the time of a secure WLAN connection.

1. Other areas, as appropriate.

 None

**References:**

[1] Internet usage worldwide - Statistics & Facts

[2] Facts and Figures 2023: Internet traffic - ITU

[3] The wireless future — ‘smarter, better, and faster’ – Cisco Systems

[4] The Commercial National Security Algorithm Suite 2.0 and Quantum Computing FAQ - NSA