P1943

Type of Project: New IEEE Standard
Project Request Type: Initiation / New
PAR Request Date: 14 Mar 2022
PAR Approval Date:
PAR Expiration Date:
PAR Status: Submitted

1.1 Project Number: P1943
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Project Title: Standard for Post-Quantum Network Security

3.1 Working Group: Post-Quantum Network Security(COM/NetSoft-SC/QuNET/WG)
3.1.1 Contact Information for Working Group Chair:
Name: Jonathan J. Attia
Email Address: jja@ieee.org
3.1.2 Contact Information for Working Group Vice Chair:
Name: Ludovic Perret
Email Address: ludovic.perret@lip6.fr
3.2 Society and Committee: IEEE Communications Society/Virtualized and Software Defined Networks, and Services Standards Committee(COM/NetSoft-SC)
3.2.1 Contact Information for Standards Committee Chair:
Name: Mehmet Ulema
Email Address: m.ulema@ieee.org
3.2.2 Contact Information for Standards Committee Vice Chair:
None
3.2.3 Contact Information for Standards Representative:
None

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE SA for Initial Standards Committee Ballot: May 2023
4.3 Projected Completion Date for Submittal to RevCom: May 2024

5.1 Approximate number of people expected to be actively involved in the development of this project: 10
5.2 Scope of proposed standard: This standard defines a method to implement optimized post-quantum version of existing network security protocols. It is based on a multi-layer protocols approach and allows data packets and/or data encapsulated to be quantum resistant to future cryptographically relevant quantum computers (CRQCs). This standard includes hybrid modes for key exchange and authentication and specifies mechanisms for handling the larger public key sizes of post-quantum algorithms. This standard excludes any definition of a new post-quantum cryptography (PQC) protocol.

5.3 Is the completion of this standard contingent upon the completion of another standard? No
5.4 Purpose: This document will not include a purpose clause.
5.5 Need for the Project: Quantum technologies are challenging today's network security: data packets are already vulnerable to future fault-tolerant quantum computing (FTQC) attacks. The current public key standards (e.g., Rivest-Shamir-Adleman known as RSA, Diffie-Hellman, Elliptic Curve Digital Signature Algorithm known as ECDSA) are not strong enough to withstand attacks using future cryptographically relevant quantum computers (CRQCs). The encrypted data with long life cycle (cf. Mosca's theorem) are at risk since they can be intercepted (data traffic) today, stored and decrypted latter once CRQCs are available. Following international recommendations, all network security protocols (e.g., Transport Layer Security known as TLS, Internet Protocol Security known as IPsec) should be upgraded to quantum-safe cryptography as soon as possible.
5.6 Stakeholders for the Standard: Telecom operators, network hardware manufacturers, network software editors, security software editors, laboratories, governmental organizations.

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? Yes

Explanation: The Security Task Group of the 802.1 Working Group considers post-quantum cryptography with a 256-bit symmetric key in accordance with NIST [1] and NSA [2]. P1913 focuses on communication between two quantum endpoints over TCP/IP (e.g., BB84 developed by Charles Bennett and Gilles Brassard in 1984). P1943 improves current network security protocols by implementing post-quantum cryptography.

7.1.1 Standards Committee Organization: C/LM
Project/Standard Number: C/LM/802.1 WG
Project/Standard Date:
Project/Standard Title: Higher Layer LAN Protocols Working Group

7.1.2 Standards Committee Organization: COM/NetSoft-SC
Project/Standard Number: P1913
Project/Standard Date:
Project/Standard Title: Software-Defined Quantum Communication

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

8.1 Additional Explanatory Notes: The National Institute of Standards and Technology (NIST) has initiated a process to solicit (announcing request for nominations for public-key post-quantum cryptographic algorithms on 12/20/2016) evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. At the time of writing, the round 3 candidates were announced July 22, 2020 (https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement) and the new standards will be defined soon by the NIST.

The expectation is that the standard will adapt the post-quantum algorithms to the IETF specifications of each protocol (adaptive update approach). Coordination with the 802.1 WG, IETF and IRTF will be considered as needed.

[1] https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs#:~:text=AES256%2DGCM%20with%20a%20random%20IV

[2] https://media.defense.gov/2021/Aug/04/2002821837/-1/-1/1/Quantum_FAQs_20210804.PDF