**P802.15.9REV1**

**Submitter Email:** kivinen@iki.fi

**Type of Project:** New IEEE Standard **PAR Request Date:** 14-May-2019 **PAR Approval Date:**

# PAR Expiration Date:

**Status:** Unapproved PAR, PAR for a New IEEE Standard

* 1. **Project Number:** P802.15.9 revision 1
  2. **Type of Document:** Standard
  3. **Life Cycle:** Full Use

**2.1 Title: IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams**

* 1. **Working Group:** Wireless Personal Area Network (WPAN) Working Group (C/LM/WG802.15)

# Contact Information for Working Group Chair Name: Robert Heile

**Email Address:** [bheile@ieee.org](mailto:bheile@ieee.org)

**Phone:** 781-929-4832

**Contact Information for Working Group Vice-Chair Name:** PATRICK KINNEY

**Email Address:** [pat.kinney@kinneyconsultingllc.com](mailto:pat.kinney@kinneyconsultingllc.com)

**Phone:** 847-960-3715

* 1. **Sponsoring Society and Committee:** IEEE Computer Society/LAN/MAN Standards Committee (C/LM)

**Contact Information for Sponsor Chair Name:** Paul Nikolich

**Email Address:** [p.nikolich@ieee.org](mailto:p.nikolich@ieee.org)

**Phone:** 8572050050

# Contact Information for Standards Representative Name: James Gilb

**Email Address:** [gilb@ieee.org](mailto:gilb@ieee.org)

**Phone:** 858-229-4822

* 1. **Type of Ballot:** Individual

# Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 03/2021

* 1. **Projected Completion Date for Submittal to RevCom:** 11/2021

DCN: 15-19-0082-02

# Approximate number of people expected to be actively involved in the development of this project: 25

* 1. **Scope:** This revision changes the 802.15.9 Recommended Practice to 802.15.9 Standard. Additionally it defines security key management extensions to address session key generation (both 128 and 256 bit key lengths), creation and/or transport of broadcast/multicast keys, and security algorithm agility. New KMPs may be added as part of this Standard. This standard is backwards compatible with 802.15.9 Recommended Practice.

# Is the completion of this standard dependent upon the completion of another standard: No

* 1. **Purpose:**
  2. **Need for the Project:** IEEE 802.15.9 Recommended Practice has been found useful for user community and making it to the standard will faciliate compliancy verification and faciliate its reference in other Standards such as 802.15.12. The IEEE 802.15.4y amendment adds support for 256-bit key lengths and the ability to select other Authenticated Encryption with Associated Data (AEAD) ciphers. Additionally, implementers of IEEE 802.15.9 needed to create their own specifications on how key material was used to create session keys. The current IEEE 802.15.9 does not include some of the KMPs emerging in the Internet of Things (IoT) market, for example (Datagram) Transport Layer Security (D)TLS 1.3 or Ephemeral Diffie-Hellman Over Concise Binary Object Representatin Objectc Signing and Encryption (EDHOC). The existing document did not address these topics for all defined KMPs when it was created leading adopting Alliances to have to create their own specifications.
  3. **Stakeholders for the Standard:** The stakeholders include silicon vendors, manufacturers and users of telecom, medical, environmental, energy, and consumer electronics equipment and manufacturers and users of equipment involving the use of wireless sensor and control networks.

# Intellectual Property

* + 1. **Is the Sponsor aware of any copyright permissions needed for this project?:** No
    2. **Is the Sponsor aware of possible registration activity related to this project?:** No

**If yes please explain:**

# Are 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):**