**P802.15.9a**

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

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

# PAR Expiration Date:

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

* 1. **Project Number:** P802.15.9 revision
  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: 06/2020

* 1. **Projected Completion Date for Submittal to RevCom:** 09/2020

DCN: 15-19-0082-00

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

* 1. **Scope:** This revision moves the 802.15.9 from Recommened Practice to Standard. During that it also defines security key management extensions to the IEEE 802.15.9 to address session key generation (both 128 and 256 bit key lengths), creation of broadcast/multicast keys plus security algorithm selection. 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. There has been also some new KMPs which might be considered to be added to this standard if there is enough interest in the group. This standard is going to be backwards compatible with the old recommended practice.

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

* 1. **Purpose:**
  2. **Need for the Project:** At the time of publication for IEEE 802.15.9, the IEEE 802.15.4 standard only supported 128 bit security keys with AES-128-CCM\*. The IEEE 802.15.4y amendment adds support for 256 bit key lengths and the ability to select other AEAD ciphers (e.g. CCM, GCM, etc.). Additionally, implementers of IEEE 802.15.9 needed to create their own specifications on how key material was used to create session keys. The existing IEEE 802.15.9 recommended practice is also silent on the topic of group key generation. It would be useful to extended IEEE 802.15.9 to cover these topics. The current IEEE 802.15.9 does not include some of the KMPs emerging in the IoT market, for example (D)TLS 1.3 or EDHOC.
  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):**