

P802.15.9

Submitter Email: bheile@ieee.org

Type of Project: Revision to IEEE Standard 802.15.9-2016

PAR Request Date: 09-Jun-2019

PAR Approval Date:

PAR Expiration Date:

Status: Unapproved PAR, PAR for a Revision to an existing IEEE Standard

1.1 Project Number: P802.15.9

1.2 Type of Document: Standard

1.3 Life Cycle: Full Use

2.1 Title: Standard for Transport of Key Management Protocol (KMP) Datagrams **Changes in title:** ~~IEEE Recommended Practice~~ Standard for Transport of Key Management Protocol (KMP) Datagrams

3.1 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

Phone: 781-929-4832

Contact Information for Working Group Vice-Chair

Name: PATRICK KINNEY

Email Address: pat.kinney@kinneyconsultingllc.com

Phone: 847-960-3715

3.2 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

Phone: 8572050050

Contact Information for Standards Representative

Name: James Gilb

Email Address: gilb@ieee.org

Phone: 858-229-4822

4.1 Type of Ballot: Individual

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

4.3 Projected Completion Date for Submittal to RevCom

Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 10/2021

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

5.2 Scope: This revision changes IEEE Std. 802.15.9 from a Recommended Practice to a 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.

Changes in scope: This ~~recommended revision practice~~ changes defines IEEE Std. 802.15.9 from a ~~message~~ Recommended exchange Practice framework to based on Standard. information. Additionally elements it (HE) defines as security a key transport management method extensions for to KMP address datagram session key generation (both 128 and guidelines 256 for bit the key use lengths), creation and/or transport of some broadcast/multicast existing keys, and security algorithm agility. New KMPs with may IEEE be added 802 as part of this Standard. 15.4 (TM). This recommended standard practice is does backwards not compatible create with a 802.15.9 new Recommended KMP Practice.

5.3 Is the completion of this standard dependent upon the completion of another standard:

5.4 Purpose: This standard describes support for transporting KMP datagrams to support the security functionality present in IEEE Std 802.15.4. Significant in support of KMP transport is the definition of a

Changes in purpose: This ~~recommended practice~~ standard describes support for transporting KMP datagrams to support the security functionality present in IEEE Std 802.15.4. Significant in support of

general purpose multiplexed (MPX) data service supporting fragmentation, re-assembly, and protocol dispatch for payloads unable to fit in a single MAC frame.

KMP transport is the definition of a general purpose multiplexed (MPX) data service supporting fragmentation, re-assembly, and protocol dispatch for payloads unable to fit in a single MAC frame.

5.5 Need for the Project: The IEEE 802.15.9 Recommended Practice has been useful for the current user community, but converting it to a standard will improve the consistency of how it is used, facilitate compliancy verification/certification, expand the community of users, and facilitate its reference and use in other Standards such as 802.15.12 draft standard for an intelligent upper layer interface (ULI) for IEEE Std 802.15.4. In addition, the IEEE 802.15.4y draft amendment for Security Next Generation is adding support for 256-bit key lengths and the ability to select other Authenticated Encryption with Associated Data (AEAD) ciphers. For this to be accomplished, supporting capability needs to be added to IEEE Std 802.15.9. Further, current implementers of IEEE Std 802.15.9 have created their own specifications on how key material should be used to create session keys, since these are not currently covered in IEEE Std 802.15.9, and the Recommended Practice 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 Representing Objects Signing and Encryption (EDHOC). This deficiency is yet another driver pushing adopting Alliances to create their own specifications. This is counter to the goal of achieving broad scale interoperability. This standard addresses that deficiency.

5.6 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

6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: No

6.1.b. Is the Sponsor 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 Joint Development

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

8.1 Additional Explanatory Notes: