

P802.15.9

Submitter Email: bheile@ieee.org

Type of Project: Modify Existing Approved PAR

PAR Request Date: 20-Jul-2015

PAR Approval Date: 03-Sep-2015

PAR Expiration Date: 31-Dec-2016

Status: Modification to a Previously Approved PAR

Root PAR: P802.15.9 **Approved on:** 07-Dec-2011

1.1 Project Number: P802.15.9

1.2 Type of Document: Recommended Practice

1.3 Life Cycle: Full Use

2.1 Title: Recommended Practice 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: 857.205.0050

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: 08/2015

4.3 Projected Completion Date for Submittal to RevCom: 02/2016

5.1 Approximate number of people expected to be actively involved in the development of this project: 100

5.2 Scope: This Recommended Practice defines a message exchange framework based on Information Elements as a transport method for key management protocol (KMP) datagrams and guidelines for the use of some existing KMPs with IEEE Std 802.15.4. This Recommended Practice does not create a new KMP.

Changes in scope: This Recommended Practice defines a message exchange framework based on Information Elements as a transport method for key management protocol (KMP) datagrams and guidelines for the use of some existing KMPs with the IEEE Std 802.15.4 and ~~IEEE Std 802.15.7~~. This Recommended Practice does not create a new KMP.

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

5.4 Purpose: This Recommended Practice describes support for transporting KMPs datagrams to support the security functionality present in IEEE Std 802.15.4

Changes in purpose: This Recommended Practice describes support for transporting KMPs datagrams to support the security functionality present in IEEE Std 802.15.4 and ~~IEEE Std 802.15.7~~.

5.5 Need for the Project: IEEE Std 802.15.4 has always supported datagram security, but has not provided a mechanism for establishing the keys used by this feature. Lack of key management support in IEEE Std 802.15.4 results in weak keys which is a common avenue for attacking the security system. Adding KMP support is critical to a proper security framework. This project will provide a Recommended Practice for the transport of KMP datagrams within these standards. It will also provide guidelines for KMPs like IETF's HIP, IKEv2, IEEE Std 802.1X, and 4-Way-Handshake.

5.6 Stakeholders for the Standard: The stakeholders include implementers and those who deploy IEEE Std 802.15.4 that need network security and thus need a mechanism for initiating and maintaining the security keys. The stakeholders include consumer electronics manufacturers, building automation, and utilities.

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?: Yes

If yes please explain: It is anticipated that a registry may be needed for KMP IDs. An initial list of KMPs and assigned IDs will be provided within the Recommended Practice. Over time, new KMPs will be developed, vetted elsewhere, then be added as supported KMPs through either an addendum to this Recommended Practice or through a KMP ID registry process.

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 (Item Number and Explanation): Reason for change:

When the project was originally started the goal was to include both 15.4 and 15.7 in the Recommended Practice.

As work proceeded, it became evident that changes were needed in 15.7 which the group had hoped might be accommodated within the time frame of this project. When the 15.7 project activity was converted to a Revision it was no longer possible to align the project timelines and it was decided to defer support for 15.7 to a later time.