P802.15.4y

Submitter Email: bheile@ieee.org
Type of Project: Amendment to IEEE Standard 802.15.4-2015
PAR Request Date: 18-Jan-2018
PAR Approval Date:
PAR Expiration Date:
Status: Unapproved PAR, PAR for an Amendment to an existing IEEE Standard

---

1.1 Project Number: P802.15.4y
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Title: Standard for Low-Rate Wireless Networks
Amendment defining security extensions to the IEEE 802.15.4 standard adding at a minimum AES-256

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: 11/2019
4.3 Projected Completion Date for Submittal to RevCom
Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 05/2020

5.1 Approximate number of people expected to be actively involved in the development of this project: 60
5.2.a. Scope of the complete standard: This standard defines the physical layer (PHY) and medium access control (MAC) sublayer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption requirements. In addition, the standard provides modes that allow for precision ranging. PHYs are defined for devices operating various license-free bands in a variety of geographic regions.

5.2.b. Scope of the project: This amendment defines security extensions to IEEE Std 802.15.4-Current Revision adding at a minimum AES-256. Defining possible simple methods of adding future encryption modes and key lengths is also explored as part of this amendment. The current IEEE Std 802.15.4-2015 supports either AES-128 or no security and adding additional modes is currently a complex process.

5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: The standard provides for ultra low complexity, ultra low cost, ultra low power consumption, and low data rate wireless connectivity among inexpensive devices. In addition, one of the alternate PHYs provides precision ranging capability that is accurate to one meter. Multiple PHYs are defined to support a variety of frequency bands.

5.5 Need for the Project: As IEEE 802.15.4 devices have become widely deployed into critical infrastructure applications, those users are now asking for a roadmap to AES-256 support and future extensions to cover, for example, Quantum Computing attacks.

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: