**P802.15.4y**

**Submitter Email:** don.sturek@itron.com

**Type of Project:** New IEEE Standard **PAR Request Date:** 18-Jan-2018 **PAR Approval Date:**

# PAR Expiration Date:

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

* 1. **Project Number:** P802.15.4y
  2. **Type of Document:** Standard
  3. **Life Cycle:** Full Use

**2.1 Title:** Security Next Generation (SECN) for IEEE 802.15.4 Low-Rate Wireless Networks

* 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: 12/2019

* 1. **Projected Completion Date for Submittal to RevCom:** 08/2020

DCN: 15-18-0037-01

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

* 1. **Scope:** This standard defines security extensions to the IEEE 802.15.4 standard to add additional encryption modes and key lengths. The current IEEE 802.15.4 standard supports either no security or AES-128. This project will at a minimum add support for AES-256 but also possibly add a capability to negotiate additional future encryption modes and key lengths.

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

* 1. **Purpose:** This standard defines a set of extensions to IEEE 802.15.4 to negotiate among a set of pre-defined encryption modes and key lengths then advertise their use in packet exchanges.
  2. **Need for the Project:** As IEEE 802.15.4 devices have become widely deployed into critical infrastructure applications, those customers are now asking for a roadmap to AES-256 support and future extensions to cover Quantum Computing attacks.
  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?:** Yes

**If yes please explain:** As noted in the scope and need for the project, this project will use EPD for multiple higher layer protocols. Values of the Multiplex ID below 1500, as defined in IEEE Std 802.15.9 Key Management Protocol, will be administered by the IEEE 802.15 Assigned Number Authority (ANA).

# 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):**

5.2:

IEEE 802.15.4: Low-Rate Wireless Networks

IEEE 802.15.9: Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams