P802.15.4ae

Type of Project: Amendment to IEEE Standard 802.15.4-2020
Project Request Type: Initiation / Amendment
PAR Request Date:
PAR Approval Date:
PAR Expiration Date:
PAR Status: Draft
Root Project: 802.15.4-2020

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

2.1 Project Title: IEEE Standard for Low-Rate Wireless Networks Amendment: Ascon cryptographic algorithms

3.1 Working Group: Wireless Specialty Networks (WSN) Working Group(C/LAN/MAN/802.15 WG)
3.1.1 Contact Information for Working Group Chair:
Name: Clinton Powell
Email Address: cpowell@ieee.org
3.1.2 Contact Information for Working Group Vice Chair:
Name: PHILIP E BEECHER
Email Address: phil@beecher.co.uk
3.2 Society and Committee: IEEE Computer Society/LAN/MAN Standards Committee(C/LAN/MAN)
3.2.1 Contact Information for Standards Committee Chair:
Name: James Gilb
Email Address: gilb_ieee@tuta.com
3.2.2 Contact Information for Standards Committee Vice Chair:
Name: David Halasz
Email Address: dave.halasz@ieee.org
3.2.3 Contact Information for Standards Representative:
Name: George Zimmerman
Email Address: george@cmephyconsulting.com

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE SA for Initial Standards Committee Ballot: Nov 2025
4.3 Projected Completion Date for Submittal to RevCom: Dec 2026

5.1 Approximate number of people expected to be actively involved in the development of this project: 10
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 in a variety of geographic regions.
5.2.b Scope of the project: Add additional cryptographic algorithms Ascon-128/Ascon-128a for the IEEE Std 802.15.4 for link encryption and authentication.

5.3 Is the completion of this standard contingent upon the completion of another standard? No
5.4 Purpose: This document will not include a purpose clause.
Change to Purpose: ~~The standard provides for ultra low complexity, ultra low cost, ultra low power consumption, and low data rate wireless connectivity among inexpensive devices, especially targeting the communications requirements of what is now commonly referred to as the Internet of Things. In addition, some of the alternate PHYs provide 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: NIST has selected Ascon as its lightweight cipher, thus providing it in the IEEE Std 802.15.4 is needed.
In addition Ascon provides functions that are not available in the Advanced Encryption Standard (AES).
5.6 Stakeholders for the Standard: The stakeholders include 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.

6.1 Intellectual Property

6.1.1 Is the Standards Committee aware of any copyright permissions needed for this project?
No

6.1.2 Is the Standards Committee 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 Is it the intent to develop this document jointly with another organization? No

---

8.1 Additional Explanatory Notes: 5.2.b Ascon-128/Ascon-128a: Ascon is a family of lightweight authenticated ciphers that had been selected by US National Institute of Standards and Technology (NIST) for future standardization of the lightweight cryptography.
Ascon provides the same Authenticated Encryption with Associated Data (AEAD) functionality as Advanced Encryption Standard (AES), allowing it to be a drop in replacement.

5.5 Ascon provides functions like hashing and extracting key material, which are not provided by AES. These functions are not currently used by IEEE Std 802.15.4, but key management protocols defined in IEEE Std 802.15.9 need such functions and providing one algorithm that supports encryption, authentication, hashing, and key material extraction allows more lightweight implementations in the future.