P802.15.9a

Type of Project: Amendment to IEEE Standard 802.15.9-2021
Project Request Type: Initiation / Amendment
PAR Request Date:
PAR Approval Date:
PAR Expiration Date:
PAR Status: Draft
Root Project: 802.15.9-2021

1.1 Project Number: P802.15.9a
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Project Title: IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams Amendment: Ephemeral Diffie-Hellman Over COSE (EDHOC) KMP

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 security key management extensions to address session key generation (both 128-bit and 256-bit key lengths), the creation and/or transport of broadcast/multicast keys, and security algorithm agility. This standard maintains backwards compatibility with IEEE Std 802.15.9-2016.
5.2.b Scope of the project: Specify the use of EDHOC (RFC 9528) KMP for the IEEE Std 802.15.9.

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: ~~This standard describes support for transporting KMP datagrams to support the security functionality present in IEEE Std 802.15.4(TM). Significant in support of 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 media access control (MAC) frame.~~
5.5 Need for the Project: Existing methods in IEEE Std 802.15.9 cannot be used without IEEE Std 802.15.9 fragmentation. EDHOC is a lightweight key management protocol whose messages can be sent in frames without fragmentation, and has a low code footprint matching the objectives for IEEE 802.15.
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.

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 Ephemeral Diffie-Hellman Over COSE (EDHOC) (RFC 9528) is a lightweight authenticated key exchange protocol standardized by the IETF following known security design and extensive security analysis. EDHOC provides analogous functionality as existing KMPs in IEEE Std 802.15.9.

5.5 EDHOC is using the Concise Binary Object Representation (CBOR, RFC 8949) for compact encoding, and the CBOR Object Signature and Encryption (COSE, RFC9052) for secure encapsulation and identification of algorithms and credentials. CBOR is designed for extremely small code size and extensibility without the need for version negotiation, properties which are in part are inherited by COSE by being specified in CBOR. These generic enablers are becoming increasingly more deployed for various purposes enabling code reuse and thereby more lightweight implementations in the future.