



BSI Standards Publication

Telecommunications and information exchange between systems — Local and metropolitan area networks specific requirements

Part 15-9: Transport of Key Management Protocol (KMP) Datagrams

National foreword

This British Standard is the UK implementation of ISO/IEC/IEEE 8802-15-9:2024.

The UK participation in its preparation was entrusted to Technical Committee IST/6, Data communications.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 32197 5
ICS 35.110

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2025.

Amendments/corrigenda issued since publication

Date	Text affected
<hr/>	



International
Standard

**ISO/IEC/IEEE
8802-15-9**

**Telecommunications and
information exchange between
systems — Local and metropolitan
area networks specific
requirements —**

**Part 15-9:
Transport of Key Management
Protocol (KMP) Datagrams**

*Télécommunications et échange d'information entre systèmes —
Réseaux locaux et métropolitains — Exigences spécifiques —*

*Partie 15-9: Transport des datagrammes du protocole de gestion
des clés (KMP)*

**First edition
2024-11**



COPYRIGHT PROTECTED DOCUMENT

© IEEE 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from IEEE at the address below.

Institute of Electrical and Electronics Engineers, Inc
3 Park Avenue, New York
NY 10016-5997, USA

Email: stds.ipr@ieee.org
Website: www.ieee.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

ISO/IEC/IEEE 8802-15-9 was prepared by IEEE (as IEEE 802.15.9:2021) and drafted in accordance with its editorial rules. It was adopted, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

A list of all parts in the ISO/IEC/IEEE 8802 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

IEEE Std 802.15.9™-2021
(Revision of IEEE Std 802.15-9-2016)

IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams

Developed by the
LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 16 June 2021

IEEE SA Standards Board

Abstract: 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™ is defined in this standard. A new KMP is not created in this standard. In support of KMP transmission and reception, a generic multiplexed data service layer that can be used to transmit large packets from the upper KMP to another peer and that provides for protocol discrimination is also provided in this standard. The multiplexed data service provides a fragmentation and multiplexing layer for those packets so they can be delivered over smaller MAC layer frames and multiplexed on the recipient end to the right processing service. The multiplexing provides for EtherType protocol discrimination.

Keywords: EtherType, fragmentation, IE, IEEE 802.15.9™, information element, key management protocol, KMP, multiplexed data service, security

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2022 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 18 January 2022. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-7720-8 STD24805
Print: ISBN 978-1-5044-7721-5 STDPD24805

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#). An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#). For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#). Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this standard was completed, the IEEE 802.15 Working Group had the following membership:

Robert F. Heile, *IEEE 802.15 Working Group Chair*

Rick Alfvén, *IEEE 802.15 Working Group Vice-Chair*

Patrick W. Kinney, *IEEE 802.15 Working Group Vice-Chair, IEEE 802.15 Working Group Secretary*

James P. K. Gilb, *IEEE 802.15 Working Group Technical Editor*

Benjamin A. Rolfe, *IEEE 802.15 Working Group Treasurer*

Tero Kivinen, *802.15.9 Chair, Technical Editor*

Peter Yee, *802.15.9 Vice Chair, Secretary*

Mounir Achir
Keiji Akiyama
Richard Alfvén
Hideki Aoyama
Arthur Astrin
Philip Beecher
Frederik Beer
Kiran Bynam
Edgar Callaway
Chris Calvert
Radhakrishna Canchi
Jaesang Cha
Kapseok Chang
Soo-Young Chang
Clint Chaplin
Stephen Chasko
Paul Chilton
Sangsung Choi
Hee-Sang Chung
Hendricus De Ruijter
Guido Dolmans
Igor Dotlic
Stefan Drude
Dietmar Eggert
Shahriar Emami
Andrew Estrada
David Evans
Kiyoshi Fukui
Matthew Gillmore
Tim Godfrey
Jussi Haapola
Shinsuke Hara
Timothy Harrington
James Hartman
Marco Hernandez

Ken Hiraga
Koji Horisaki
Iwao Hosako
Bing Hui
Yeong Min Jang
Seong-Soon Joo
Hyunduk Kang
Shuzo Kato
Toyoyuki Kato
Jeritt Kent
Jaehwan Kim
Junhyeong Kim
Youngsoo Kim
Shoichi Kitazawa
Ryuji Kohno
Fumihide Kojima
Thomas Kuerner
Byung-Jae Kwak
Hoosung Lee
Jae Seung Lee
Moon-Sik Lee
Myung Lee
Huan-Bang Li
Liang Li
Qing Li
Michael Lynch
Itaru Maekawa
Hiroyuki Matsumura
Michael Mc Laughlin
Michael McInnis
Kenichi Mori
Robert Moskowitz
Mohammad Nekoui
Chiu Ngo

Paul Nikolich
John Notor
Hiroyo Ogawa
Mitsuaki Oshima
Chandrashekhar P S Bhat
Park Taejoon
Glenn Parsons
Charles Perkins
Albert Petrick
Clinton Powell
Verotiana Rabarijaona
Demir Rakanovic
Ivan Reede
RobertsRichard
Behcet Sarikaya
Noriyuki Sato
Norihiko Sekine
Nikola Serafimovski
Kunal Shah
Stephen Shellhammer
Shusaku Shimada
Masashi Shimizu
Gyung Chul Sihm
Gary Stuebing
Don Sturek
Mineo Takai
Kou Togashi
Kiyoshi Toshimitsu
Murat Uysal
Billy Verso
Gabriel Villardi
Brian Weis
Makoto Yaita
Yu Zeng
Chunhui Zhu

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Robert Aiello	Raj Jain	Thomas Starai
Philip E. Beecher	Pranav Jha	Walter Struppler
Vern Brethour	Piotr Karocki	Gary Stuebing
William Byrd	Stuart Kerry	Gerald Stueve
Paul Cardinal	Yongbum Kim	Don Sturek
Pin Chang	Tero Kivinen	Mark Sturza
Suresh Channarasappa	Yasushi Kudoh	Mark-Rene Uchida
Michael Cowan	Hyeon Ho Lee	Dmitri Varsanofiev
Hendricus De Ruijter	Rajesh Murthy	Billy Verso
Donald Dunn	Bansi Patel	Xiaohui Wang
Liu Fangfang	Arumugam Paventhan	Lisa Ward
Avraham Freedman	Clinton Powell	Scott Willy
Hongmei He	Maximilian Riegel	Andreas Wolf
Marco Hernandez	Robert Robinson	Chun Yu Charles Wong
Werner Hoelzl	Benjamin Rolfe	Yu Yuan
Klaus Hueske	Naotaka Sato	Oren Yuen
	Kunal Shah	

When the IEEE SA Standards Board approved this standard on 16 June 2021, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy	Howard Li	Mehmet Ulema
Doug Edwards	Daozhuang Lin	Lei Wang
Ramy Ahmed Fathy	Kevin Lu	F. Keith Waters
J. Travis Griffith	Daleep C. Mohla	Karl Weber
Thomas Koshy	Chenhui Niu	Sha Wei
Joseph L. Koepfinger*	Damir Novosel	Howard Wolfman
David J. Law	Annette Reilly	Daidi Zhong
	Dorothy Stanley	

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.15.9™-2021, IEEE Standard for Transport of Key Management Protocol (KMP) Datagrams.

Key management has been recognized as critical component for network security, but IEEE Std 802.15.4™ does not provide any methods for key management and leaves it out of scope. So this standard was created to provide a methodology to enable key management by providing a transport for key management protocols (KMPs) outside the application layers.

The first revision of the 802.15.9-2016 was a Recommended Practice, and this revision of the 802.15.9 will change it to an IEEE Standard.

The scope of the 2016 version of IEEE Std 802.15.9 was as follows:

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.

The current scope of IEEE Std 802.15.9-2021 is as follows:

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.

Contents

1.	Overview.....	12
1.1	General.....	12
1.2	Scope.....	12
1.3	Purpose.....	12
1.4	Deprecated features.....	12
1.5	Word usage	12
2.	Normative references	13
3.	Definitions, acronyms, and abbreviations.....	13
3.1	Definitions	13
3.2	Acronyms and abbreviations	13
4.	Introduction.....	14
4.1	Overview.....	14
4.2	System view.....	15
4.3	Network view.....	16
4.4	Security associations.....	16
4.5	Process flow	16
4.6	State machine	17
4.7	Address formats	17
4.8	KMP payload size	17
4.9	Format conventions.....	17
5.	MPX data service.....	17
5.1	Description.....	17
5.2	MPX data primitives.....	18
5.3	MPX-PURGE primitive.....	25
5.4	MPX PIB attributes.....	27
6.	KMP transport service	27
6.1	Overview.....	27
6.2	KMP-CREATE primitives.....	28
6.3	KMP-FINISHED primitives.....	33
6.4	KMP-DELETE primitives	35
6.5	KMP-PURGE primitives	37
7.	MPX IE format	39
7.1	IE overview	39
7.2	Payload IE group ID	39
7.3	MPX IE content	39
8.	KMP Service.....	43
8.1	KMP ID.....	43
8.2	Vendor-specific KMPs	43

9.	State machines	44
9.1	Inbound state machine	44
9.2	Outbound state machine.....	46
Annex A (informative) KMP specifics—IEEE 802.1X/MKA		47
A.1	Description.....	47
A.1.1	Device authentication	47
A.1.2	Device authentication and cryptographic key agreement.....	48
A.2	Use cases.....	51
A.2.1	Overview	51
A.2.2	Isolated enclave	52
A.2.3	Star topology	52
A.2.4	Mesh	52
A.3	IEEE 802.15 specifics.....	52
A.3.1	EAPOL message framing.....	52
A.3.2	EAPOL-MKA	52
A.3.3	EAPOL-KEY	54
A.3.4	ETSI TS 102 887-2	54
A.3.5	Group Traffic Key Generation	54
Annex B (informative) KMP specifics—IKEv2		56
B.1	Description.....	56
B.2	Use cases.....	56
B.2.1	General	56
B.2.2	Minimal IKEv2 use cases.....	56
B.2.3	Enterprise or large-scale IKEv2 use cases	57
B.3	IKEv2 and IEEE 802.15 specifics	57
B.3.1	Overview	57
B.3.2	Supported IKEv2 features	57
B.3.3	Unused IKEv2 features	57
B.3.4	Message framing	57
B.3.5	Algorithm negotiation	58
B.3.6	Key derivation	58
B.3.7	Broadcast and multicast key distribution	58
Annex C (informative) KMP specifics—HIP		59
C.1	Description.....	59
C.2	Use cases.....	59
C.2.1	General	59
C.2.2	Isolated enclave	59
C.2.3	Home net	60
C.2.4	City net	60
C.2.5	RFID networks	60
C.2.6	Infrastructure sensor nets.....	60
C.3	IEEE 802.15TM specifics.....	60
C.3.1	Message framing	60
C.3.2	Key derivation and security PIB interaction	60
C.3.3	Deployment recommendations.....	60
C.3.4	HIT authentication.....	61

Annex D (informative) KMP specifics—PANA	62
D.1 Description	62
D.2 Use cases	62
D.3 IEEE 802.15 specifics	62
Annex E (informative) KMP specifics—Dragonfly	65
E.1 Description	65
E.1.1 General	65
E.1.2 Device authentication	65
E.1.3 Device authentication and cryptographic key establishment	65
E.2 Use cases	67
E.3 Dragonfly and IEEE 802.15 specifics	67
E.3.1 Overview	67
E.3.2 Algorithm negotiation	68
E.3.3 Key derivation	68
E.3.4 Message framing	68
E.3.5 Broadcast and multicast key distribution	69
Annex F (informative) IEEE 802.15.4 security	70
F.1 Description	70
F.2 Link keys	70
F.3 Group keys	71
F.3.1 Overview	71
F.3.2 Key Identifier Mode 0x01	71
F.3.3 Key Identifier Mode 0x02	71
F.3.4 Key Identifier Mode 0x03	72
Annex G (informative) Bibliography	73

IEEE Standard for Transport Key Management Protocol (KMP) Datagrams

1. Overview

1.1 General

This document defines a standard for the transport of key management protocols (KMP) for WPANs.

1.2 Scope

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.

1.3 Purpose

This standard describes support for transporting KMP datagrams to support the security functionality present in IEEE Std 802.15.4™.¹ 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.

1.4 Deprecated features

This standard deprecates the use of PANA KMP defined in the Clause D.

1.5 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).^{2,3}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

¹Information on references can be found in Clause 2.

²The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

³The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 802.15.4™, IEEE Standard for Low-Rate Wireless Networks.^{4, 5}

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.⁶

extended address: The address as specified in 7.1 of IEEE Std 802.15.4-2020.

key management protocol (KMP): A collection of data transactions that provide the mechanism to manage cryptographic keys. This includes dealing with the generation, exchange, storage, use, and replacement of keys.

3.2 Acronyms and abbreviations

4WH	4-Way Handshake
ACL	access control list
AAA	authentication, authorization and accounting
AP	access point
AS	authentication server
BEX	base exchange
CAK	connectivity association key
DEX	diet exchange
EAP	extensible authentication protocol
EAPOL	EAP over LAN
GKH	Gate Key Handshake
HI	host identity

⁴IEEE publications are available from the Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>).

⁵The IEEE standards referred to in Clause 2 are trademarks belonging to the Institute of Electrical and Electronics Engineers, Inc.

⁶IEEE Standards Dictionary Online is available at: <http://dictionary.ieee.org>. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page..

HIP	host identity protocol
HIT	host identity tag
ICV	integrity check value
IE	information element
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IP	Internet protocol
IPsec	IP Security
KDF	key derivation function
KMP	key management protocol
MAC	media access control
MSDU	MAC Service Data Unit
MKA	MACsec key agreement
MPX	multiplexed
MPDU	MAC protocol data unit
MSK	master session key
N2N	node to node
PAN	personal area network
PANA	protocol for carrying authentication for network access
PHY	physical layer
PIB	personal area network information base
PRF	pseudo-random function
SA	security association
SPI	security parameter index
UDP	user datagram protocol
WPAN	wireless personal area network

4. Introduction

4.1 Overview

IEEE Std 802.15.4 supports datagram security, but does not specify how keys are managed. A variety of proprietary, non-interoperable approaches for key management have been implemented. This standard defines KMP approaches which meet the critical needs of an effective security framework.

This standard specifies the transportation of KMP datagrams within IEEE Std 802.15.4. It also provides guidelines for KMPs such as the Internet Engineering Task Force's (IETF) host identity protocol (HIP) (Moskowitz [B19]), Internet Key Exchange version 2 (IKEv2) (Kaufman, et al. [B16]), Protocol for carrying Authentication for Network Access (PANA) (Forsberg, et al. [B6]), Dragonfly, and IEEE Std 802.1X™ [B12].⁷

IEEE Std 802.15.4y™ [B14] provides a mechanism for using other encryption algorithms in the IEEE Std 802.15.4 than AES-CCM-128. Depending on the KMP to be used this standard can be used to negotiate the algorithm.

⁷The numbers in brackets correspond to those of the bibliography in Annex G.

This standard also provides a generic MPX data service layer that can be used to transmit large packets from the upper layer process to another peer. The MPX data service provides a fragmentation and multiplexing layer for those packets so they can be delivered over smaller MAC layer frames and multiplexed on the recipient end to the right processing service.

4.2 System view

The KMP protocol is intended to operate over a variety of wireless physical layers (PHYs). Within the family of PHYs available in the IEEE Std 802.15.4, some PHYs provide low data rates and limited PHY packet sizes. Even when the PHY layer supports large frames, there are benefits for fragmenting the packets to smaller frames. In some KMPs supported by this document the message size exceeds even the largest PHY packet size supported by any PHY defined in IEEE Std 802.15.4. For these reasons, fragmentation and reassembly of the KMP messages is essential. An interoperable fragmentation/reassembly mechanism is described in this document.

The key transport mechanism described in this document sits between the MAC services and higher layers and is shown in Figure 1.

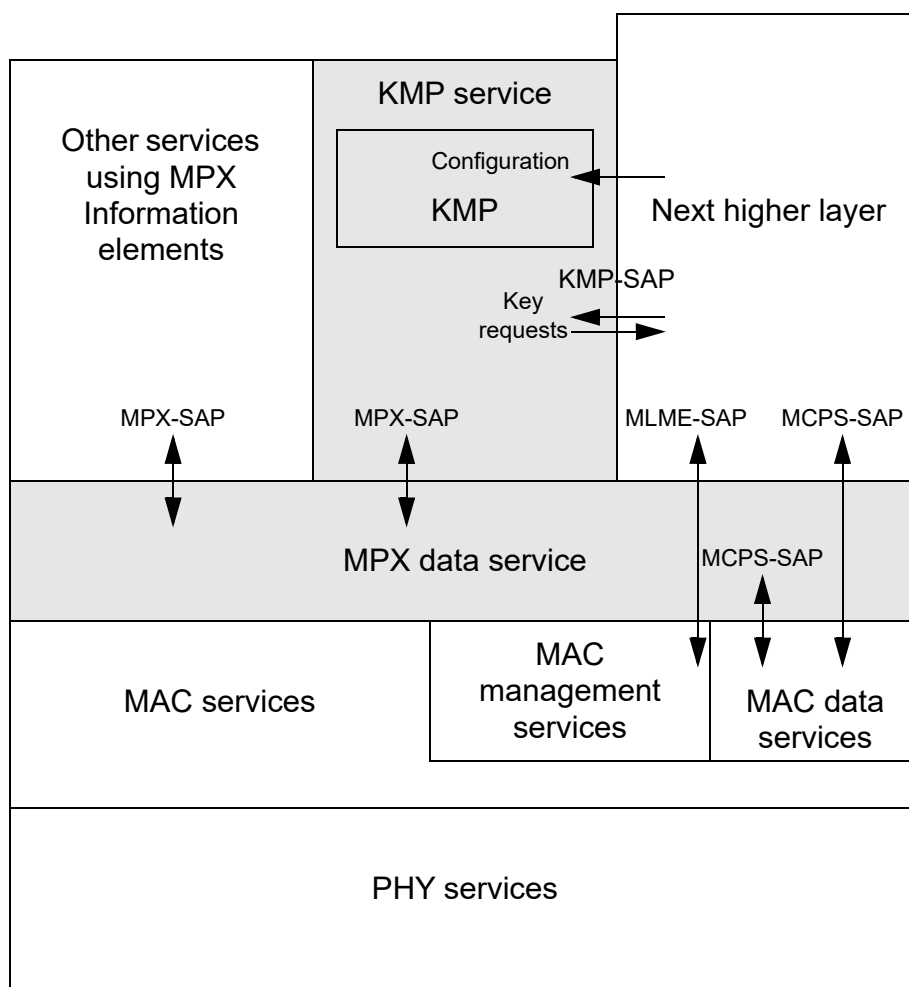


Figure 1—System overview

MPX data service provides the way to fragment and multiplex packets sent by the layers above it and send them out using the MAC data service. The interface between the MPX data service and the layers above it includes the MultiplexID and the payload to be sent or the payload received. The KMP Service will use MPX-DATA primitives to send and receive packets, and the next higher layer will talk to the KMP services through the KMP primitives.

The actual KMP is inside the KMP services, and the configuration of the KMP is provided by the next higher layer using a mechanism that is outside the scope of this document. The keys generated and the algorithms negotiated by the KMP are sent to the next higher layer, which will then install them to the MAC sublayer. The exact format of the keys and configuration depends on the KMP used, and is outside the scope of this document.

4.3 Network view

The KMP transport services are limited by the fragmentation/reassembly multiplexing service defined in this standard. The fragmentation defined in this document is intended for operation between two direct peer devices. This means that if applied to a multi-hop network topology, it is intended that fragmentation and reassembly be performed hop by hop.

The KMPs themselves are all capable of working over a multi-hop transport. If an implementation can ensure all KMP payloads fit in a single MAC protocol data unit (MPDU), the fragmentation/reassembly mechanism is not engaged. Further, the KMPs are normally used on lossy environments, and they have to work even when frames are lost, thus the lack of a multi-hop acknowledgment is not a limitation. Therefore if there is also a MAC forwarding mechanism, the KMP transport services will work in a multi-hop environment. It is up to the implementation to make sure that these constraints are met before using in a multi-hop environment.

The KMPs used by this standard may provide both link and group key management support.

4.4 Security associations

The security information between two devices is maintained in a security association (SA). The role of a KMP is to set up and maintain an SA between two or more devices. SAs may be unicast or group SAs.

Many types of SAs are possible as described in the security-related MAC personal area network (PAN) information base (PIB) attributes in 9.5 of IEEE Std 802.15.4-2020. An implementer of this standard will select from the options allowed to request the KMP higher layer to establish the desired SA and provide the necessary keys to the MAC PIB attribute. Short summary of the types of SAs in IEEE Std 802.15.4 can be found from Annex F.

4.5 Process flow

SAs can be established when a device joins the PAN, or any time prior to the first secured data transmission. There are different methods that can trigger the SA establishment. One is that the PIB *macSecurityEnabled* is set to TRUE in either device.

In a beaconing PAN, either device configured to require security may start the KMP. A coordinator may require SA establishment prior to association or the next step after association. A joining device may attempt SA establishment prior or after association if it is configured to only communicate over a secured link.

In a non-beaconing PAN, if the sender of the initial data transmission is configured to require security it first establishes the SA by starting the KMP. If the recipient is configured to require security and receives a non-secured data transmission, it drops the data transmission and starts the KMP to establish the SA.

4.6 State machine

There are separate inbound and outbound processing state machines (see Clause 9).

4.7 Address formats

To be able to send or receive a packet securely, IEEE Std 802.15.4 requires that the originator and the recipient of the frame know the extended address (see IEEE Std 802.15.4) of the other end. This means that before any link keys between peers can be established, they need to know the extended address of the originator, as the SA will be associated with that. The KMPs can use that 64-bit extended address to identify the peer and use it to authenticate the other end.

4.8 KMP payload size

As the MPX data layer allows a KMP payload to be fragmented into a maximum of 256 fragments, this means that even if the PHY is using 127 octet PHY service data units (96 octets effective fragment size), this standard can use KMP payloads up to 24 576 octets. The Total Upper Layer Frame Size field of the MPX IE is two octets, thus regardless of the maximum size of the underlying PHY the maximum KMP payload size is 65 535 octets.

4.9 Format conventions

This document follows the formatting conventions as defined in Clause 4 of IEEE Std 802.15.4-2020.

5. MPX data service

5.1 Description

The MPX data service provides a mechanism to carry multiple payloads of different higher layer services between two MAC entities, and multiplexing and fragmenting those payloads so they can be transmitted using MAC frames. The MPX data service delivers an MPX data payload from a higher protocol layer by fragmenting it into a number of MAC frames at the originator and sending them sequentially to the recipient. At the recipient, the MPX data payload is reassembled from the sequence of MAC frames and delivered to the higher protocol layer. The MPX data payload carried within MPX IEs can be sent within either Data or Multipurpose frames.

As MPX data service payloads may exceed the size of an MPDU, a fragmentation method using the MAC acknowledgment provides the needed fragmentation support. The use of the MAC acknowledgment allows the originator to be assured the receiving device has all the frames to reassemble the MPX data service payload. Retransmission of unacknowledged frames is handled by the MAC. The MPX data service shall limit each MPX IE Content field to at maximum of *macMpxMaxFragmentSize* octets.

If the originator fails to send the data frame (for example because of the NO_ACK error status), the MPX data service shall fail the transaction and return an error to the next higher layer. As quite often there is no possibility to signal a state of failed transfer via the MAC, the recipient state machine uses a timeout defined by the *macMpxReassemblyTimeout* to determine when the originator has failed the transfer. In the MPX data service there is signaling mechanism allowing either end to request that the transfer be aborted. Recipient may request transfer to be aborted if it does not have enough resources to finish the transaction, and recipient may indicate the maximum size of transaction recipient can process in the abort message.

If a fragment is received out of order, the inbound fragmentation processing of the receiving device may be declared as failed and the transaction terminated. It is possible for the MAC layer to have acknowledged receipt of a fragment that is later dropped by a higher layer function (due to overload or lack of resources). Thus, the acknowledgment should only be taken to indicate that the fragment was received by the recipient, not that the recipient passed the fragment to the reassembly service and onto the service using the MPX IEs.

The following primitives, summarized in Table 1, are used by an entity at a higher layer to fragment and transfer an MPX payload to a remote device where it is reassembled and passed to the next higher layer.

Table 1—Summary of MPX primitives

Name	Request	Indication	Response	Confirm
MPX-DATA	5.2.2	5.2.4	—	5.2.3
MPX-PURGE	5.3.2	—	—	5.3.3

5.2 MPX data primitives

5.2.1 MPX data primitive use

Figure 2 shows a successful transfer of a payload, which must be split into three fragments for transmission by the MAC on the originator and is received and reassembled at the recipient. Figure 2 shows the next higher layer on the originator initiating the transfer by issuing the MPX-DATA.request primitive. At the recipient, on successful reassembly of the fragments into the full payload, the recipient next higher layer is signaled that a new payload has arrived using the MPX-DATA.indication. To complete the transfer, the originator next higher layer which started the transfer is signaled that the transfer completed successfully using the MPX-DATA.confirm with a status code of SUCCESS.

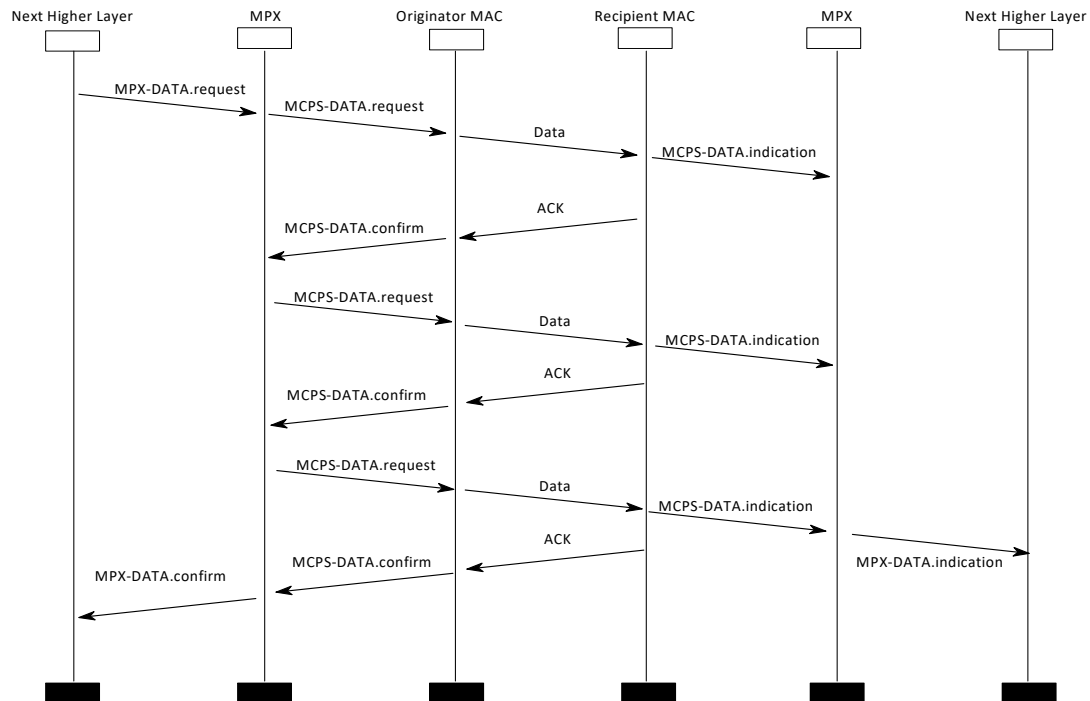


Figure 2—Message sequence for successful transfer of three fragments

Figure 3 shows an unsuccessful transfer of a fragmented payload. The figure shows the next higher layer on the originator initiating the transfer by issuing the MPX-DATA.request primitive. The transfer of the first fragment completes successfully as denoted by the ACK and MCPS-DATA.confirm. The second fragment is lost during transmission. The originator MAC (as shown in Figure 3) will try retransmitting the frame until it reaches the maximum number of retransmissions, at which point it will return failure; the MCPS-DATA.confirm returns a status of NO_ACK and the MPX-DATA.confirm carries the status to the originator next higher layer. After returning the NO_ACK status to the upper layer, the MPX data service can also optionally send an MPX IE with an abort code to inform the other end that it has aborted the transaction. As the other peer was not responding to the Acks, it is most likely because it is not in radio range, so it is quite likely that this abort message will not reach the other end either, so it is often sent without asking for Ack, and without retransmissions. If the other end receives the abort, it can immediately clear out its state. If the recipient does not receive the abort it shall drop the transaction after timeout specified by the *macMpxReassemblyTimeout* PIB attribute.

Figure 4 shows a case where the recipient cannot process the request and thus it aborts it by sending a separate Data frame having an MPX IE with an abort code. The MPX IE may also include the maximum transfer size which is then given to the originator's next higher layer along with the TRANSACTION_ABORTED status code. When receiving the MPX IE with Transfer type of aborted the Originator MAC can find matching transaction by matching the Source and Destination addresses and the Transaction ID.

In Figure 5 the recipient is configured not to accept any of the MPX IE transactions, thus it can immediately answer with the MPX IE inside the Enh-Ack it is sending back to the originator for the first fragment.