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

Reference number
ISO/IEC/IEEE 8802-15-9:2024(en)

© IEEE 2022

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.

Copyright © 2022 IEEE. All rights reserved.

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.

Copyright © 2022 IEEE. All rights reserved.

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.

Copyright © 2022 IEEE. All rights reserved.

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 Alfvin, *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 Alfvin
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 Sihn
Gary Stuebing
Don Sturek
Mineo Takai
Kou Togashi
Kiyoshi Toshimitsu
Murat Uysal
Billy Verso
Gabriel Villardi
Brian Weis
Makoto Yaita
Yu Zeng
Chunhui Zhu

Copyright © 2022 IEEE. All rights reserved.

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

Robert Aiello
Philip E. Beecher
Vern Brethour
William Byrd
Paul Cardinal
Pin Chang
Suresh Channarasappa
Michael Cowan
Hendricus De Ruijter
Donald Dunn
Liu Fangfang
Avraham Freedman
Hongmei He
Marco Hernandez
Werner Hoelzl
Klaus Hueske

Raj Jain
Pranav Jha
Piotr Karocki
Stuart Kerry
Yongbum Kim
Tero Kivinen
Yasushi Kudoh
Hyeong Ho Lee
Rajesh Murthy
Bansi Patel
Arumugam Paventhan
Clinton Powell
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Naotaka Sato
Kunal Shah

Thomas Starai
Walter Struppler
Gary Stuebing
Gerald Stueve
Don Sturek
Mark Sturza
Mark-Rene Uchida
Dmitri Varsanofiev
Billy Verso
Xiaohui Wang
Lisa Ward
Scott Willy
Andreas Wolf
Chun Yu Charles Wong
Yu Yuan
Oren Yuen

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
Doug Edwards
Ramy Ahmed Fathy
J. Travis Griffith
Thomas Koshy
Joseph L. Koepfinger*
David J. Law

Howard Li
Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Chenhui Niu
Damir Novosel
Annette Reilly
Dorothy Stanley

Mehmet Ulema
Lei Wang
F. Keith Waters
Karl Weber
Sha Wei
Howard Wolfman
Daidi Zhong

*Member Emeritus

Copyright © 2022 IEEE. All rights reserved.

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.

Copyright © 2022 IEEE. All rights reserved.

Contents

Copyright © 2022 IEEE. All rights reserved.

Copyright © 2022 IEEE. All rights reserved.

Copyright © 2022 IEEE. All rights reserved.

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*).

[1] Information on references can be found in Clause 2.

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

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

Copyright © 2022 IEEE. All rights reserved.

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]

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

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

Copyright © 2022 IEEE. All rights reserved.