

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

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997
USA

IEEE Std 802.15.9™-2016

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

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

Approved 3 March 2016
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™ are defined in the recommended practice. A new KMP is not created in this recommended practice. 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 is also provided in this recommended practice. 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.

Keywords: 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 © 2016 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 17 August 2016. 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 978-1-5044-0790-8 STD20855
Print: ISBN 978-1-5044-0791-5 STDPD20855

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 documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

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

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE-SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute 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 does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. 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: PROCUREMENT OF 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 should be considered 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, or 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 his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide 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 revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

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 imply 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.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. 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 appropriate fee, 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. 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 subject to review at least every ten years. When a document is more than ten 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 the IEEE-SA Website at http://iee.org/publications_standards/index.html or contact IEEE at the address listed previously. For more information about the IEEE-SA or IEEE's standards development process, visit the IEEE-SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: <http://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

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 <http://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.

Participants

At the time this standard was completed, the IEEE 802.15 working group had the following membership:

IEEE 802.15 Working group

Robert F. Heile, *Working Group Chair*

Rick Alfvin, *Working Group Vice-Chair*

Patrick Kinney, *Working Group Vice-Chair, Working Group Secretary*

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

Benjamin A. Rolfe, *Working Group Treasurer*

Robert Moskowitz, *802.15.9 Chair*

Peter Yee, *802.15.9 Vice Chair, Secretary*

Esko Vesala, *802.15.9 Technical Editor*

Keiji Akiyama
Hideki Aoyama
Tuncer Baykas
Philip Beecher
Monique Brown
Edgar Callaway
Chris Calvert
Radhakrishna Canchi
Jaesang Cha
Soo-Young Chang
Clint Chaplin
Stephen Chasko
Sangsung Choi
Hee-Sang Chung
Hendricus De Ruijter
Guido Dolmans
Andrew Estrada
David Evans
Kiyoshi Fukui
Tim Godfrey
Yoshiho Goto
Jussi Haapola
Shinsuke Hara
Marco Hernandez
Ken Hiraga
Jay Holcomb
Koji Horisaki
Iwao Hosako

Bing Hui
Yeong Jang
Seong-Soon Joo
Volker Jungnickel
Jeritt Kent
Jaehwan Kim
Junhyeong Kim
Shoichi Kitazawa
Tero Kivinen
Ryuji Kohno
Fumihide Kojima
Keitarou Kondou
Thomas Kuerner
Amarjeet Kumar
Byung-Jae Kwak
Namtuan Le
Jae Lee
Moon-Sik Lee
Myung Lee
Huan-Bang Li
Liang Li
Michael Lynch
Itaru Maekawa
Hiroyuki Matsumura
Michael McInnis
Kenichi Mori
Mohammad Nekoui
Chiu Ngo
Trang Nguyen

Paul Nikolich
Makoto Noda
John Notor
Mitsuaki Oshima
Glenn Parsons
Charles Perkins
Albert Petrick
Clinton Powell
Verotiana Rabarijaona
Demir Rakanovic
Ivan Reede
Richard Roberts
Noriyuki Sato
Norihiro Sekine
Nikola Serafimovski
Kunal Shah
Stephen Shellhammer
Shusaku Shimada
Gary Stuebing
Don Sturek
Mineo Takai
Kou Togashi
Kiyoshi Toshimitsu
Billy Verso
Brian Weis
Hidetoshi Yokota
Yu Zeng
Junwen Zhang

Major contributions were received from the following individuals:

Riccardo Brama
Chris Calvert
David Evans
Rene Hummen
Piotr Karocki

Toyoyuki Kato
Tero Kivinen
Glenn Parsons
Verotiana Rabarijaona
Benjamin A. Rolfe

Michael Seaman
Kunal Shah
Shusaku Shimada
Rene Struik
Angela Thomas

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

Rick Alfvén	Noriyuki Ikeuchi	Clinton Powell
Butch Anton	Akio Iso	Venkatesha Prasad
Philip Beecher	Atsushi Ito	Verotiana Rabarijaona
Harry Bims	Raj Jain	Karen Randall
Gennaro Boggia	Adri Jovin	Maximilian Riegel
Riccardo Brama	Shinkyō Kaku	Robert Robinson
Nancy Bravin	Piotr Karocki	Benjamin A. Rolfe
Susan Burgess	Jeritt Kent	Bartien Sayogo
William Byrd	Stuart Kerry	Michael Seaman
Juan Carreon	Yongbum Kim	Kunal Shah
Minho Cheong	Patrick Kinney	Shusaku Shimada
Keith Chow	Tero Kivinen	Thomas Starai
Charles Cook	Bruce Kraemer	Rene Struik
Sourav Dutta	Yasushi Kudoh	Walter Struppler
Peter Ecclesine	Thomas Kurihara	Gerald Stueve
Richard Edgar	Arthur H. Light	Don Sturek
Liu Fangfang	Elvis Maculuba	Mark Sturza
Avraham Freedman	Edward McCall	Mark-Rene Uchida
Devon Gayle	Michael McInnis	Lorenzo Vangelista
James P. K. Gilb	Robert Moskowitz	Dmitri Varsanofiev
Tim Godfrey	Michael Newman	Raj Vaswani
Randall Groves	Nick S. A. Nikjoo	George Vlantis
Robert F. Heile	Paul Nikolich	Karl Weber
Marco Hernandez	John Notor	Hung-Yu Wei
Werner Hoelzl	Yoshihiro Ohba	Brian Weis
Tetsushi Ikegami	Satoshi Oyama	Oren Yue
	Dalibor Pokrajac	

When the IEEE-SA Standards Board approved this standard on 4 March 2016, it had the following membership:

Jean-Philippe Faure, *Chair*
Ted Burse, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Chuck Adams	Ronald W. Hotchkiss	Mehmet Ulema
Masayuki Ariyoshi	Michael Janezic	Yingli Wen
Stephen Dukes	Joseph L. Koepfinger*	Howard Wolfman
Jianbin Fan	Hung Ling	Don Wright
J. Travis Griffith	Kevin Lu	Yu Yuan
Gary Hoffman	Annette D. Reilly	Daidi Zhong
	Gary Robinson	

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.15.9™-2016, IEEE Recommended Practice 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 recommended practice was created to provide a methodology to enable key management by providing a transport for key management protocols (KMPs) outside the application layers.

Contents

1.	Overview.....	12
1.1	Scope.....	12
1.2	Purpose.....	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	System view.....	14
4.2	Network view.....	16
4.3	Security associations.....	16
4.4	Process flow.....	16
4.5	State machine.....	16
4.6	Address formats.....	17
4.7	KMP payload size.....	17
4.8	Format conventions.....	17
5.	MPX data service.....	17
5.1	Description.....	17
5.2	MPX data primitives.....	18
5.2.1	MPX-DATA.request	21
5.2.2	MPX-DATA.confirm	23
5.2.3	MPX-DATA.indication	24
5.3	MPX-PURGE primitives.....	26
5.3.1	MPX-PURGE.request	26
5.3.2	MPX-PURGE.confirm	27
6.	KMP transport service.....	28
6.1	KMP-CREATE primitives.....	29
6.1.1	KMP-CREATE.request	30
6.1.2	KMP-CREATE.confirm	31
6.1.3	KMP-CREATE.indication	31
6.1.4	KMP-CREATE.response	32
6.2	KMP-FINISHED primitives.....	33
6.2.1	KMP-FINISHED.indication	33
6.3	KMP-DELETE primitives.....	34
6.3.1	KMP-DELETE.request	34
6.3.2	KMP-DELETE.confirm	35
6.3.3	KMP-DELETE.indication	36
6.4	KMP-PURGE primitives.....	37
6.4.1	KMP-PURGE.request	37
6.4.2	KMP-PURGE.confirm	38

7.	MPX IE format	38
7.1	Payload IE group ID	38
7.2	MPX IE content	39
7.2.1	Transaction Control field	39
7.2.2	Total Upper-Layer Frame Size field	41
7.2.3	Multiplex ID field	41
7.2.4	Upper-Layer Frame Fragment field	42
8.	KMP Service	42
8.1	Vendor-specific KMPs	42
9.	State machines	43
9.1	Inbound state machine	43
9.2	Outbound state machine	45
Annex A (informative) KMP specifics—IEEE 802.1X/MKA		46
A.1	Description	46
A.1.1	Device authentication	46
A.1.2	Device authentication and cryptographic key agreement	47
A.2	Use cases	50
A.2.1	Isolated enclave	50
A.2.2	Star topology	50
A.2.3	Mesh	51
A.3	IEEE 802.15 specifics	51
A.3.1	EAPOL message framing	51
A.3.2	EAPOL-MKA	51
A.3.3	EAPOL-KEY	52
A.3.4	ETSI TS 102 887-2	53
Annex B (informative) KMP specifics—IKEv2		54
B.1	Description	54
B.2	Use cases	54
B.2.1	Minimal IKEv2 use cases	54
B.2.2	Enterprise or large-scale IKEv2 use cases	55
B.3	IKEv2 and IEEE 802.15 specifics	55
B.3.1	Supported IKEv2 features	55
B.3.2	Unused IKEv2 features	55
B.3.3	Message framing	55
B.3.4	Algorithm negotiation	55
B.3.5	Key derivation	56
B.3.6	Broadcast and multicast key distribution	56

Annex C (informative) KMP specifics—HIP	57
C.1 Description.....	57
C.2 Use cases.....	57
C.2.1 Isolated enclave.....	57
C.2.2 Home net.....	57
C.2.3 City net.....	58
C.2.4 RFID networks.....	58
C.2.5 Infrastructure sensor nets	58
C.3 IEEE 802.15TM specifics.....	58
C.3.1 Message framing.....	58
C.3.2 Key derivation and security PIB interaction.....	58
C.3.3 Deployment recommendations	58
C.3.4 HIT authentication	59
Annex D (informative) KMP specifics—PANA	60
D.1 Description.....	60
D.2 Use cases.....	60
D.3 IEEE 802.15 specifics.....	60
Annex E (informative) KMP specifics—Dragonfly	63
E.1 Description.....	63
E.1.1 Device authentication	63
E.1.2 Device authentication and cryptographic key establishment.....	63
E.2 Use cases.....	65
E.3 Dragonfly and IEEE 802.15 specifics.....	65
E.3.1 Algorithm negotiation.....	66
E.3.2 Key derivation.....	66
E.3.3 Message framing.....	66
E.3.4 Broadcast and multicast key distribution.....	67
Annex F (informative) KMP specifics—IEEE 802.15.4 security	68
F.1 Description.....	68
F.2 Link keys.....	68
F.3 Group keys.....	69
F.3.1 Key Identifier Mode 0x01.....	69
F.3.2 Key Identifier Mode 0x02.....	69
F.3.3 Key Identifier Mode 0x03.....	70
Annex G (informative) Bibliography	71

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

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers 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.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading “Important Notice” or “Important Notices and Disclaimers Concerning IEEE Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/TPR/disclaimers.html>.

1. Overview

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

1.1 Scope

This recommended practice defines a message exchange framework based on information elements (IE) as a transport method for KMP datagrams and guidelines for the use of some existing KMPs with IEEE Std 802.15.4^{TM1}. This recommended practice does not create a new KMP.

1.2 Purpose

This recommended practice describes support for transporting KMP datagrams to support the security functionality present in IEEE Std 802.15.4. 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 MAC frame.

¹Information on references can be found in Clause 2.

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.^{2, 3}

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.⁴

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
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

²IEEE publications are available from the Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>.)

³The IEEE standards referred to in Clause 2 are trademarks belonging to the Institute of Electrical and Electronics Engineers, Inc.

⁴*IEEE Standards Dictionary Online* subscription is available at: <http://ieeexplore.ieee.org/xpls/dictionary.jsp>.

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
PKIX	public-key infrastructure (X.509)
PRF	pseudo-random function
PSDU	PHY service data unit
SA	security association
SPI	security parameter index
UDP	user datagram protocol
WPAN	wireless personal area network

4. Introduction

IEEE Std 802.15.4 has always supported datagram security, but has not provided a mechanism for establishing the keys used by this feature. Lack of key management support has resulted in a variety of proprietary, non-interoperable, sometimes poorly secured approaches for key management. Adding KMP support is critical to a proper security framework.

This recommended practice specifies the transportation of KMP datagrams within these standards. It also provides guidelines for KMPs such as the Internet Engineering Task Force's (IETF) host identity protocol (HIP) (Moskowitz [B18]), Internet Key Exchange version 2 (IKEv2) (Kaufman, et al. [B14]), Protocol for carrying Authentication for Network Access (PANA) (Forsberg, et al. [B5]), Dragonfly (Annex E as used in IEEE Std 802.11sTM [B12]), and IEEE Std 802.1XTM [B9]⁵.

This recommended practice 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.

4.1 System view

The KMP protocol is intended to operate over a variety of wireless PHYs. Within the family of PHYs available in the reference standards, some provide low data rates and limited PHY packet sizes; under some environmental conditions the transmission of large packets over the wireless medium, even when supported by the PHY packet structure, is unlikely to be successful. In some KMPs supported by this document the message size exceeds even the largest PHY packet size supported by any PHY defined in the reference standards. For these reasons, fragmentation and reassembly of the KMP messages is essential. An interoperable fragmentation/reassembly mechanism is described in this document.

⁵The numbers in brackets correspond to those of the bibliography in Annex G.

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

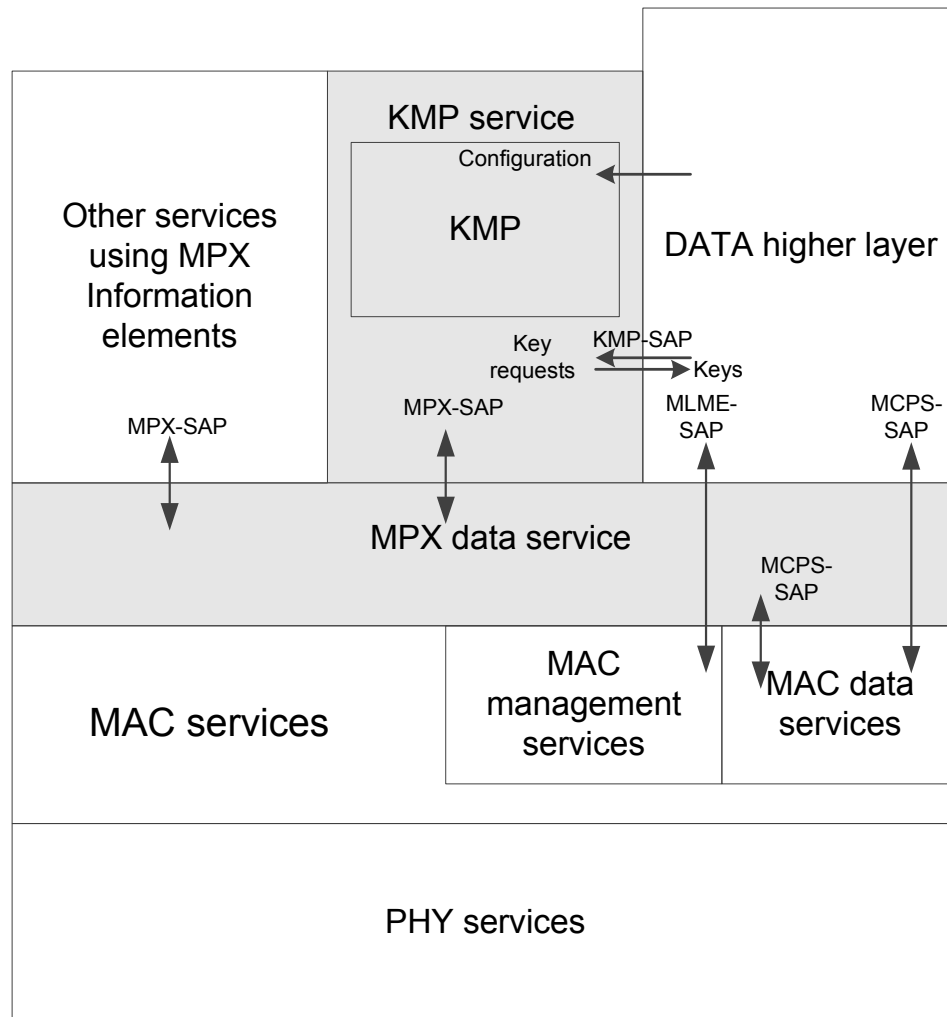


Figure 1—System overview

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 DATA higher layer will talk to the KMP services through the KMP primitives. MLME-SAP is not used.

The actual KMP is inside the KMP services, and the configuration of the KMP is provided by the DATA higher layer using a mechanism that is outside the scope of this document. The keys generated by the KMP are sent to the DATA 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.

4.2 Network view

The KMP transport services are limited by the fragmentation/reassembly multiplexing service defined in this recommended practice. 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 internally handle lost messages, 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 KMP services provided here can provide both link and group key management support.

4.3 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 a 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 information base (PIB) attributes in 9.5 of IEEE Std 802.15.4. An implementer of this recommended practice 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.

4.4 Process flow

SAs can be established in a beaconing PAN when a device joins the PAN, or in a non-beaconing PAN, just prior to the first secured data transmission. There are different methods that can trigger the SA establishment. One is that the PIB *macSecurityEnabled* is 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 receiver is configured to require security and receives a non-secured data transmission, it shall drop the data transmission and start the KMP to establish the SA.

4.5 State machine

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

4.6 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 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 them to authenticate the other end.

4.7 KMP payload size

As the MPX data layer allows a KMP payload to be fragmented up to 256 fragments, this means that even if the PHY is using 127 octet PSDUs (96 octets effective fragment size), this recommended practice can use KMP payloads up to 24 576 octets.

4.8 Format conventions

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

5. MPX data service

5.1 Description

The MPX data service provides a mechanism to carry payloads between multiple different higher layer services between two nodes connected by a MAC link, and multiplexing and fragmenting those payloads so they can be transmitted using MAC frames. The data payloads provided to the MPX data service are typically larger than the size that will fit in a single MAC frame. The MPX data service delivers a 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 within the MAC and is not apparent to the user of the MPX data service. The receiving side must anticipate duplicate frames to accommodate the case where an acknowledgment frame is lost and the frame is retransmitted. This behavior is accommodated within the receiving state machine.

If the originator fails to send the frame (for example because of the TRANSACTION_EXPIRED error status), the MPX data service will 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 receiver state machine uses a timeout on receiving the next expected frame in the chain to determine when the originator has failed the transfer. There is a signaling mechanism allowing either end to request that the transfer be aborted. Recipient might request transfer to be aborted if it does not have enough resources to finish it, and it might indicate the maximum size of transaction it can process in the abort message.

The mechanism described in this specification does not try to handle out of order fragments, e.g., if a fragment is lost (i.e., the inbound state machine registers a skipped fragment), the inbound processing fails; this is considered an acceptable behavior. Further, it is possible for the MAC layer to have acknowledged receipt of a fragment that is later dropped by a higher layer function (overload or lack of resources). Thus, the acknowledgment should only be taken to indicate that the fragment made it to the recipient, not that the recipient passed the fragment to the reassembly service and onto the service using the MPX IEs.

5.2 MPX data primitives

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

Table 1—Summary of MPX primitives

Name	Request	Indication	Response	Confirm
MPX-DATA	5.2.1	5.2.3		5.2.2
MPX-PURGE	5.3.1			5.3.2

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 receiver. The figure shows the next higher layer on the originator initiating the transfer by issuing the MPX-DATA.request primitive. At the receiver, on successful reassembly of the fragments into the full payload, the receiver 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.

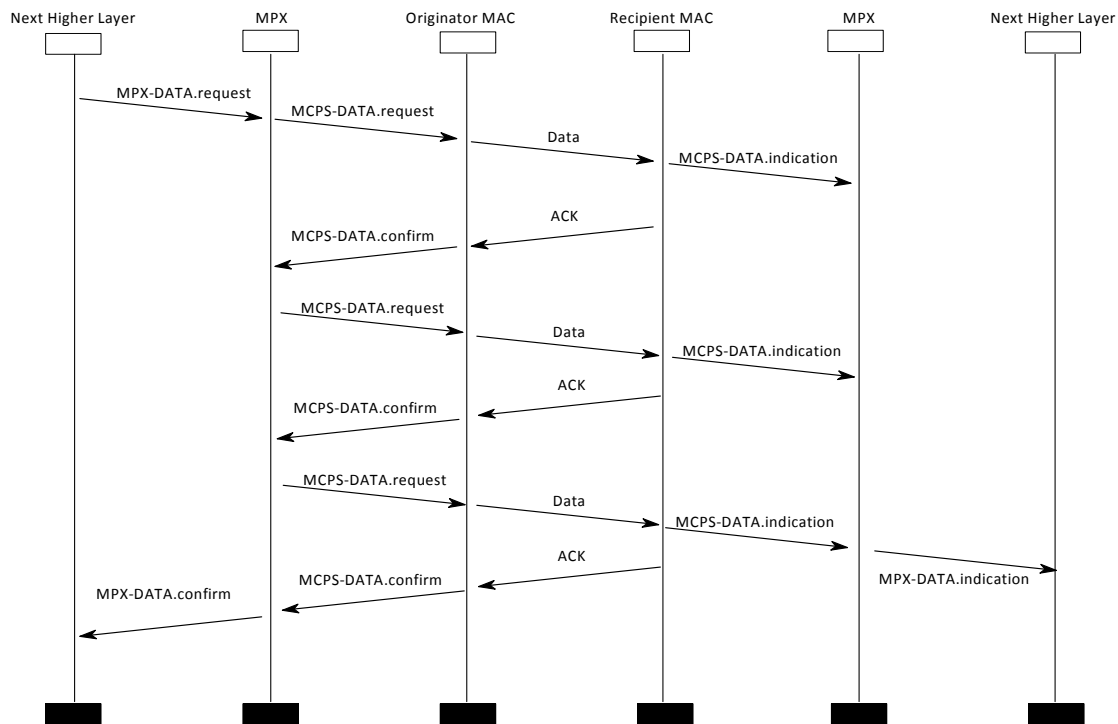


Figure 2—Message sequence for successful transfer of three fragments

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 TRANSACTION_EXPIRED and the MPX-DATA.confirm carries the status to the originator next higher layer. After returning the TRANSACTION_EXPIRED status to the upper layer, the MPX layer 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 should be sent without asking for Ack, and without retransmissions. If the other end receives the abort, it can immediately clear out its state.

Figure 4 shows a case where the recipient cannot process the request and thus it aborts it by sending separate a Data frame having an MPX IE with an abort code. The MPX IE might also include the maximum transfer size which is then given to the originator's next higher layer along with the TRANSACTION_ABORTED status code.

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.

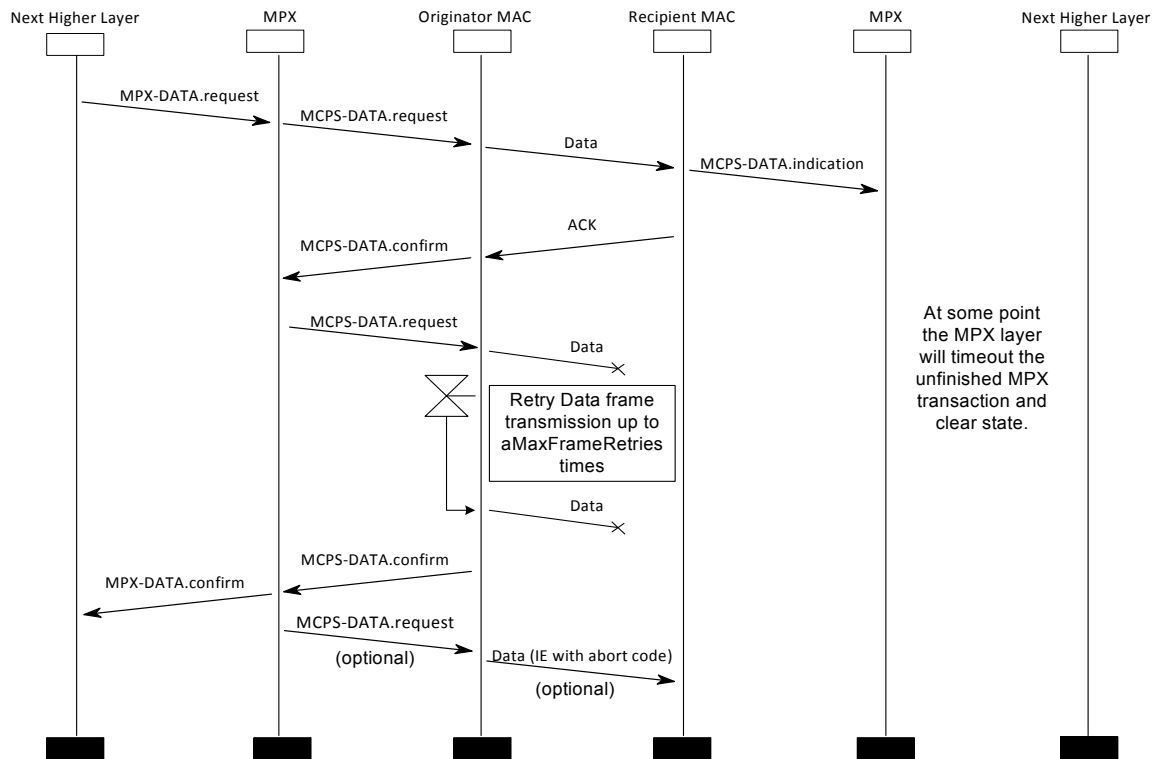


Figure 3—Failed fragment transfer

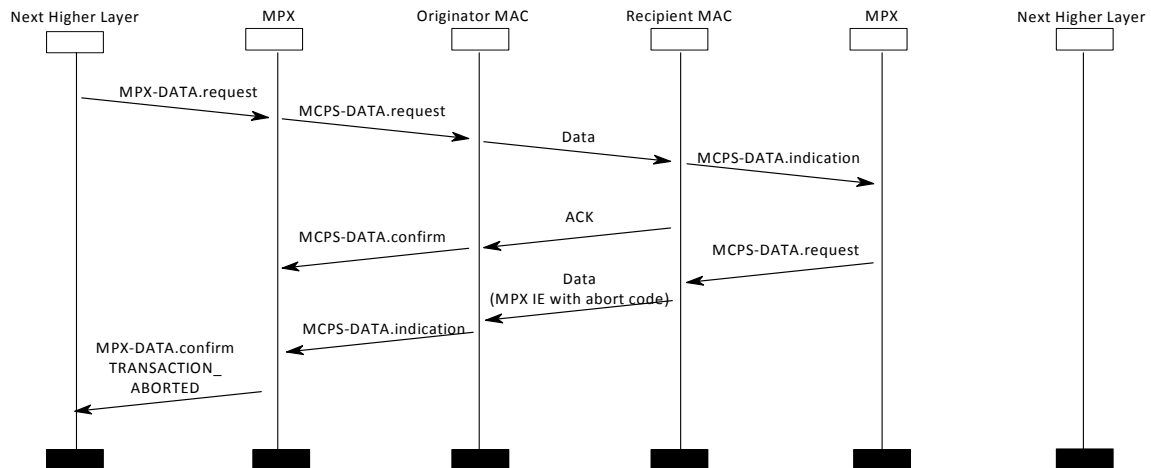


Figure 4—Aborted fragment transfer

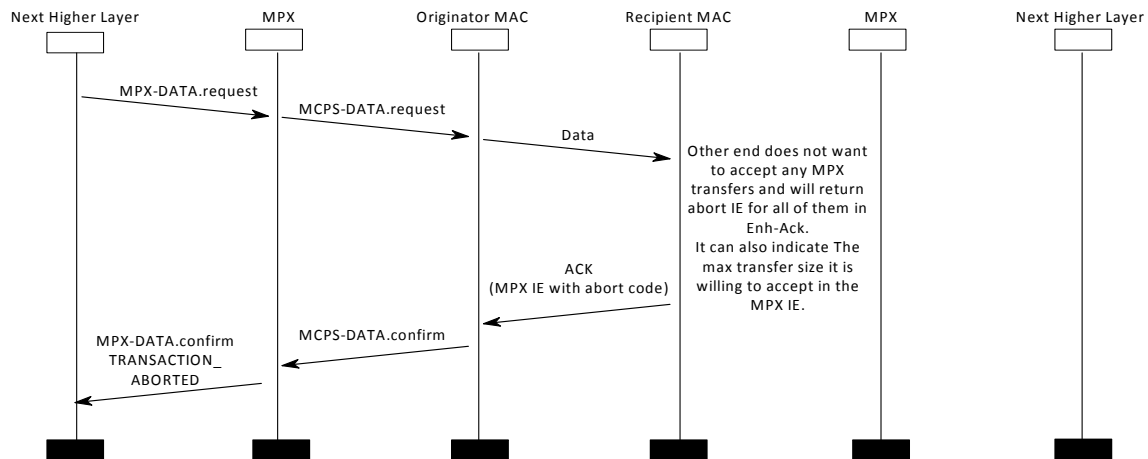


Figure 5—Aborted fragment transfer in Enh-Ack

5.2.1 MPX-DATA.request

The MPX-DATA.request primitive requests the transfer of a MPX payload to another device.

The semantics of this primitive are as follows:

```
MPX-DATA.request (
    SrcAddrMode,
    DstAddrMode,
    DstPanId,
    DstAddr,
    MultiplexId,
    MpxDataMpxData,
    MpxHandle,
    SecurityLevel,
    KeyIdMode,
    KeySource,
    KeyIndex,
    SendMultipurpose
)
```

The primitive parameters are described in Table 2.

Table 2—MPX-DATA.request parameters

Name	Type	Valid range	Description
SrcAddrMode	Enumeration	NONE, SHORT, EXTENDED	The source addressing mode for this MPX data.
DstAddrMode	Enumeration	NONE, SHORT, EXTENDED	The destination addressing mode for this MPX data.
DstPanId	Integer	0x0000–0xffff	The PAN identifier of the entity to which the MPX data is being transferred.
DstAddr	—	As specified by the DstAddrMode parameter.	The address of the receiving (destination) device.
MultiplexId	Integer	0x0000–0xffff	The higher-layer protocol using the MPX data service. See 7.2.3.
MpxData	Set of octets	—	The set of octets forming the MPX data payload.
MpxHandle	Integer	0x00–0xff	An identifier which can be used to refer to the particular primitive transaction; used to match a confirm primitive with the corresponding request.
SecurityLevel	Integer	0–7	The combination of Message Integrity Check and Encryption to be applied to the payload of the MPX data service. For encoding see Table 9-6 in IEEE Std 802.15.4.
KeyIdMode	Integer	As defined in Table 9-7 of IEEE Std 802.15.4.	The mode used to identify the key purportedly used by the originator of the received frame. This parameter is invalid if the SecurityLevel parameter is set to 0x00.
KeySource	Set of octets	As indicated by the KeyIdMode parameter.	The originator of the key purportedly used by the originator of the received frame. The KeySource field, when present, indicates the originator of a group key. If the Key Identifier Mode field indicates a 4-octet Key Source field, then the Key Source field shall be the <i>macPanId</i> of the originator of the group key right concatenated with the <i>macShortAddress</i> of the originator of the group key. If the Key Identifier Mode field indicates an 8 octet Key Source field, then the Key Source field shall be set to the <i>macExtendedAddress</i> of the originator of the group key. This parameter is invalid if the KeyIdMode parameter is invalid or set to 0x00 or set to 0x01.