INTERNATIONAL STANDARD

ISO/IEC/ IEEE 8802-1X

First edition
2013-12-01
AMENDMENT 1
2016-02-15

Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks —

Part 1X: Port-based network access control

AMENDMENT 1: MAC security key agreement protocol (MKA) extensions

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux locaux et métropolitains — Exigences spécifiques —

Partie 1X: Contrôle d'accès au réseau basé sur le port

AMENDEMENT 1: Extensions du protocole d'accord de clés de sécurité MAC

Reference number
ISO/IEC/IEEE 8802-1X:2013/Amd.1:2016(E)

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1
© IEEE 2014

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat, the IEC Central Office and IEEE do not accept any liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies and IEEE members. In the unlikely event that a problem relating to it is found, please inform the ISO Central Secretariat or IEEE at the address given below.

COPYRIGHT PROTECTED DOCUMENT

© IEEE 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from ISO, IEC or IEEE at the respective address below.

ISO copyright office
Case postale 56
CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
E-mail inmail@iec.ch
Web www.iec.ch

Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York
NY 10016-5997, USA
E-mail stds.ipr@ieee.org
Web www.ieee.org

Published in Switzerland

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.
© IEEE 2014 – All rights reserved
Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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.

The main task of ISO/IEC JTC 1 is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is called to the possibility that implementation of this standard may require the use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. ISO/IEEE is not responsible for identifying essential patents or patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents or patent claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance or a Patent Statement and Licensing Declaration Form, 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 ISO or the IEEE Standards Association.

Amendment 1 to ISO/IEC/IEEE 8802-1X:2013 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE 802.1Xbx-2014). It was adopted by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in parallel with its approval by the ISO/IEC national bodies, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE. IEEE is responsible for the maintenance of this document with participation and input from ISO/IEC national bodies.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1
© IEEE 2014 – All rights reserved

(blank page)

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.1Xbx™-2014
(Amendment to
IEEE Std 802.1X™-2010)

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

IEEE Std 802.1Xbx™-2014
(Amendment to
IEEE Std 802.1X™-2010)

IEEE Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 10 December 2014

IEEE-SA Standards Board

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Abstract: Media Access Control security (MACsec) Key Agreement protocol (MKA) data elements and procedures that provide additional security and manageability capabilities, including the ability to maintain secure communication while the operation of MKA is suspended, when used in conjunction with MACsec Cipher Suites that support Extended Packet Numbering are added in this amendment.

Keywords: authorized port, confidentiality, data origin authenticity, IEEE 802.1X™, IEEE 802.1Xbx™, integrity, LANs, local area networks, MAC Bridges, MAC security, MAC Service, MANs, metropolitan area networks, port based network access control, secure association, security, transparent bridging

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

Copyright © 2014 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 22 December 2014. 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 978-0-7381-9435-6** **STD20045**
Print: **ISBN 978-0-7381-9436-3** **STDPD20045**

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.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

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.

Documents
Document Sharing Hub

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

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.

Documents
Document Sharing Hub

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Photocopies

Subject to payment of the 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 subjected 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://ieeexplore.ieee.org/xpl/standards.jsp 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 all IEEE standards can be accessed on the IEEE-SA Website 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 at 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.

Documents
Document Sharing Hub

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Participants

At the time this amendment was submitted to the IEEE-SA Standards Board for approval, the IEEE 802.1 Working Group had the following membership:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
Mick Seaman, *Security Task Group Chair, Editor*

Ting Ao
Christian Boiger
Paul Bottorff
David Chen
Feng Chen
Weiying Cheng
Diego Crupnicoff
Rodney Cummings
Patrick Diamond
Aboubacar Kader Diarra
Janos Farkas
Norman Finn
Geoffrey Garner
Anoop Ghanwani
Mark Gravel
Eric W. Gray
Craig Gunther
Stephen Haddock
Hitoshi Hayakawa
Jeremy Hitt
Rahil Hussain
Tony Jeffree
Michael Johas Teener
Peter Jones
Hal Keen
Marcel Kiessling
Yongbum Kim
Philippe Klein
Jouni Korhonen
Jeff Lynch
Ben Mack-Crane
Christophe Mangin
James McIntosh
Eric Multanen
Donald Pannell
Karen Randall
Maximilian Riegel
Dan Romascanu
Jessy V. Rouyer
Panagiotis Saltsidis
Behcet Sarikaya
Daniel Sexton
Johannes Specht
Kevin B. Stanton
Wilfried Steiner
Vahid Tabatabaee
Patricia Thaler
Jeremy Touve
Karl Weber
Yuehua Wei
Brian Weis
Jordon Woods
Juan-Carlos Zuniga

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

Thomas Alexander
Butch Anton
Olugbenga Ayinde
William Byrd
Juan Carreon
Keith Chow
Charles Cook
Grazia Delia
Sourav Dutta
Richard Edgar
Yukihiro Fujimoto
Devon Gayle
Gregory Gillooly
Randall Groves
Michael Gundlach
Werner Hoelzl
Atsushi Ito
Tony Jeffree
Peter Jones
Shinkyo Kaku
Piotr Karocki
Stuart Kerry
Max Kicherer
Jeff Koftinoff
Bruce Kraemer
Yasushi Kudoh
Thomas Kurihara
Paul Lambert
Hyeong Ho Lee
Shen Loh
Elvis Maculuba
Jouni Malinen
Michael Newman
Nick S.A. Nikjoo
Satoshi Obara
Satoshi Oyama
Karen Randall
Maximilian Riegel
Jessy V. Rouyer
Mick Seaman
Kapil Sood
Thomas Starai
Rene Struik
Walter Struppler
Joseph Tardo
William Taylor
Patricia Thaler
Dmitri Varsanofiev
Hung-Yu Wei
Brian Weis
Oren Yuen
Daidi Zhong

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.
Documents
Document Sharing Hub
Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

When the IEEE-SA Standards Board approved this amendment on 10 December 2014, it had the following membership:

John Kulick, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Peter Balma
Farooq Bari
Ted Burse
Clint Chaplain
Stephen Dukes
Jean-Phillippe Faure
Gary Hoffman
Michael Janezic
Jeffrey Katz
Joseph L. Koepfinger*
David J. Law
Hung Ling
Oleg Logvinov
Ted Olsen
Glenn Parsons
Ron Peterson
Adrian Stephens
Peter Sutherland
Yatin Trivedi
Phil Winston
Don Wright
Yu Yuan

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
Michael Janezic, *NIST Representative*

Catherine Berger
IEEE-SA Content Production and Management

Kathryn Bennett
Program Manager, IEEE-SA Technical Program Operations

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Introduction

This introduction is not part of IEEE Std 802.1Xbx™-2014, IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control—Amendment 1: MAC Security Key Agreement Protocol (MKA) Extenstions.

This first amendment to IEEE Std 802.1X-2010, extends MKA to realize additional security and manageability capabilities made possible by the IEEE Std 802.1AEbw™ amendment that added extended packet numbering Cipher Suites to IEEE Std 802.1AE™-2006. Secure connectivity association (CA) members can now temporarily suspend MKA operation without causing protocol timeouts that would disrupt secure data transfer, thus allowing in-service control plane software upgrades.

The first edition of IEEE Std 802.1X was published in 2001. The second edition, IEEE Std 802.1X-2004 clarified areas related to mutual authentication and the interface between IEEE 802.1X specified state machine, and those specified by the Extensible Authentication Protocol (EAP), and by IEEE Std 802.11™ in support of IEEE Std 802.1X.

The third edition, IEEE Std 802.1X-2010, added authenticated key agreement in support of IEEE Std 802.1AE™ MAC Security, clarifying and generalizing the relationship between the common architecture specified for port-based network access control, and the functional elements and protocols that support that architecture as specified in IEEE Std 802.1X, other IEEE 802® standards, and in IETF RFCs. Further changes updated the standard to reflect best current practice, insisting, for example, upon mutual authentication methods and using such methods in examples. A greater emphasis was placed on the security of systems accessing the network, as well as upon the security of the network accessed, and some prior provisions, with a more comprehensive treatment of segregating and limiting connectivity to unauthenticated systems. Applications of port-based network access that use IEEE Std 802.1AE MAC Security (MACsec) and/or MKA (MACsec Key Agreement protocol) are described.

Every effort was made to ensure that systems conformant to IEEE Std 802.1X-2010 will interoperate, without prior configuration, with implementations conforming to IEEE Std 802.1X-2004 and IEEE Std 802.1X-2001. However it is anticipated that claims of conformance in respect of some existing implementations, not needing to support IEEE Std 802.1AE and already conforming to best current practice as of 2010, will continue to refer to IEEE Std 802.1X-2004. IEEE Std 802.1X-2010 includes a number of improvements to the specification of the port access control protocol (PACP) state machines and their relationship to EAP methods and state machines.

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.
Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Contents

2.Normative references 2

3.Definitions 5

4.Abbreviations and acronyms 6

5.Conformance 7

5.11 MKA options 7

6.Principles of port-based network access control operation 8

6.2 Key hierarchy 8

7.Port-based network access control applications 9

9.MACsec Key Agreement protocol (MKA) 10

9.1 Protocol design requirements 10
9.5 Key server election 14
9.8 SAK generation, distribution, and selection 16
9.15 MKA participant timer values 17
9.16 MKA management 17
9.18 In-service upgrades 18
9.19 In-service upgrade examples 22

11.EAPOL PDUs 26

11.5 EAPOL protocol version handling 26
11.11 EAPOL-MKA 26

12.PAE operation 32

12.1 Model of operation 32
12.2 KaY interfaces 32
12.5 Logon Process 33
12.9 PAE management 34

13.PAE MIB 36

13.4 Security considerations 36
13.5 Definitions for PAE MIB 36

Annex A (normative) PICS Proforma 85

A.9 MKA requirements and options 85

Annex B (informative) Bibliography 86

Annex H (informative) Test vectors 88

H.1 KDF 88
H.2 CAK Key Derivation 89
H.3 CKN Derivation 89
H.4 KEK Derivation 90

Documents
Document Sharing Hub

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

H.5 ICK Derivation 90
H.6 SAK Derivation 91

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Figures

Figure 11-10 MACsec SAK Use parameter set 29
Figure 11-12 Distributed SAK parameter set (other MACsec Cipher Suites) 29
Figure 11-13 Distributed CAK parameter set 30
Figure 11-16 XPN parameter set 30
Figure 12-3 PAE management information 35

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Tables

Table 9-1 MKA Algorithm Agility parameter values 12
Table 9-3 MKA Participant timer values 17
Table 11-7 MKPDU parameter sets 27
Table 13-4 PAE managed object cross-reference table 36
Table 13-4 PAE managed object cross-reference table 36

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.
Documents
Document Sharing Hub
Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

IEEE Standard for
Local and metropolitan area networks—

Port Based Network Access Control

Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions

[This amendment is based on IEEE Std 802.1X™-2010.]

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strikethrough~~ (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Deletions and insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.

IIMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, security, 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/IPR/disclaimers.html.

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub
Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

2. Normative references

Change the Normative references clause as follows:

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 802.1D™, IEEE Standard for Local and Metropolitan Area Networks: Media access control (MAC) Bridges.[1, 2]

IEEE Std 802.1Q™, IEEE Standard for Local and Metropolitan Area Networks: Bridges and Bridged Networks ~~Virtual Bridged Local Area Networks~~.

IEEE Std 802.1AB™, IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity and Discovery.

~~IEEE Std 802.1ad™-2005, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.~~

IEEE Std 802.1AE™, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.

IEEE Std 802.1AE™-2006, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.[3]

IEEE Std 802.1AEbn™-2011, IEEE Standard for Local and Metropolitan Area Network — Media Access Control (MAC) Security — Amendment 1: Galois Counter Mode—Advanced Encryption Standard—256 (GCM–AES–256) Cipher Suite.

IEEE Std 802.1AEbw™-2013, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security — Amendment 2: Extended Packet Numbering.

IEEE Std 802.1AX™, IEEE Standard for Local and Metropolitan Area Networks: Link Aggregation.

IEEE Std 802.2™, 1998 Edition [ISO/IEC 8802-2: 1998], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.[4]

IEEE Std 802.3™, IEEE Standard for Ethernet~~Information technology—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications~~.

---

[1]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA. IEEE publications can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

[2]The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[3]This standard refers to the latest edition of IEEE Std 802.1AE in addition to referencing specific revisions and amendments.

[4]ISO [IEEE] and ISO/IEC [IEEE] documents are available from ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA. ISO [IEEE] and ISO/IEC [IEEE] documents can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

IEEE Std 802.11™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

IEEE Std 802.17™-2004 IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 17: Resilient packet ring (RPR) access method and physical layer specifications.

IEEE Std 802.1AR™, IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identifier.

IETF RFC 2578, STD 58, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.[5]

IETF RFC 2579, STD 58, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2580, STD 58, Conformance Statements for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2863, The Interfaces Group MIB using SMIv2, McCloghrie, K. and Kastenholz, F., June 2000.

~~IETF RFC 2869, RADIUS Extensions, Rigney, C., Willats, W., and Calhoun, P., June 2000.~~

IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, J. Schaad, R. Housley, September 2002.

~~IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework, J. Case, R. Mundy, D. Partain, B. Stewart, December 2002.~~

~~IETF RFC 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), Aboba, B., Calhoun, P., September 2003.~~

~~IETF RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Guidelines, Congdon, P., Aboba, B., Smith, A., Zorn, G., Roese, J., September 2003.~~

IETF RFC 3629, STD 63, UTF-8, a transformation format of ISO 10646, Yergeau, F., November 2003.

~~IETF RFC 4017, Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, Stanley, D., Walker, J., Aboba, B., March 2005.~~

IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, Diercks, T., Rescorla, E., April 2006.

IETF RFC 4493, THE AES-CMAC Algorithm, Song, J.H., Lee, J., Iwata, T., June 2006.

~~IETF RFC 4675, RADIUS Attributes for Virtual LAN and Priority Support, Congdon, P., Sanchez, M., Aboba, B., September 2006.~~

IETF RFC 5216, The EAP-TLS Authentication Protocol, Simon, D., Aboba, B., Hurst, R., March 2008.

[5]IETF RFCs are available from the Internet Engineering Task Force website at http://www.ietf.org/rfc.html.

Documents
Document Sharing Hub

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

IETF RFC 5247, Extensible Authentication Protocol (EAP) Key Management Framework, Aboba, B., Simon, D., Eronen, P., October 2007.

~~FIPS Publication 197, The Advanced Encryption Standard (AES), U.S. DoC/NIST, November 26, 2001.~~

ISO/IEC 18033-3: 2010, Information technology—Security techniques—Encryption algorithms—Part 3:Block ciphers.

~~NIST Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules[6], 3 December 2002.~~

~~NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, May 2005.[7]~~

~~NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, E. Barker, J. Kelsey, revised March 2007.~~

NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, Lily Chen, November 2008.

[6] ~~National Institute of Standards and Technology, FIPS 140-2 is available at http://www.nist.gov/cmvp.~~

[7] NIST Special Publications (800 Series) are available at http://csrc.nist.gov/publications/PubsSPs.html.

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

3. Definitions

Change the definition of packet number as follows:

packet number (PN): A monotonically increasing value ~~used to uniquely identify a MACsec frame in the sequence of frames transmitted using an SA~~ that is guaranteed unique for each MACsec frame transmitted using a given SAK.

Insert the following definition(s), in the appropriate collating order:

extended packet number (XPN): A 64-bit packet number (PN) specified in IEEE Std 802.1AE.

Salt: A 96-bit secret value communicated by key agreement protocol for use by the protection and verification operations of the IEEE Std 802.1AE GCM-AES-XPN Cipher Suites.

Short Secure Channel Identifier (SSCI): A 32-bit value that is unique for each SCI within the context of all SecYs using a given SAK.

NOTE—IEEE Std 802.1AEbw-2013 specifies the calculation of SSCI and Salt values used by the IEEE Std 802.1AE GCM-AES-XPN Cipher Suites from other MKA values.

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

4. Abbreviations and acronyms

Insert the following abbreviation(s), in the appropriate collating sequence:

SSCI	Short SCI
XPN	Extended Packet Number

Delete the following abbreviation:

FDDI	Fiber Distributed Data Interface

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

5. Conformance

5.11 MKA options

Insert new subclause 5.11.4 as follows:

5.11.4 In-service upgrades

A PAE that supports in-service upgrades shall be capable of

a) Suspending MKA operation as specified in 9.18.
b) Communicating the values of the most significant 32 bits of the Lowest Acceptable PN for the Latest Key and the Old Key when any XPN capable Cipher Suite is being used, as specified in 9.18.5.

NOTE—Selection and use of Extended Packet Numbering depends on the implementation of an XPN capable Cipher Suite by each SecY participating in a CA. See IEEE Std 802.1AE as amended by IEEE Std 802.1AEbw-2013.

A PAE that supports in-service upgrades may use additional protocol(s), outside the scope of this specification, to coordinate in-service upgrades as specified in 9.18.6.

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

6. Principles of port-based network access control operation

6.2 Key hierarchy

Change the first paragraph of 6.2 as follows:

The root key in the MACsec Key Agreement key hierarchy is the Connectivity Association Key (CAK), and is identified by a CAK Name (CKN). MKA (Clause 9) does not use the CAK directly but derives two further keys from the CAK using the AES cipher (~~FIPS Publication 197~~ISO/IEC 18033-3) in CMAC mode (9.3). These are the ICV Key (ICK) used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, and the Key Encrypting Key (KEK) used by Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a CA. See Figure 6-3.

Change 6.2.4 as follows:

6.2.4 Algorithm agility

To accommodate future developments in cryptography, MKA provides an explicit Algorithm Agility parameter (9.3.3, 11.11.2, Figure 11-8). The Algorithm Agility parameter identifies the following:

a) How the ICV is derived from the CAK and the data of a given MKPDU; and
b) How a CAK is derived from the parameters available to the participants in an EAP exchange.

Knowledge of item a) is required for MKA's use of CAKs in general, while both item a) and item b) are required for the validation of MKPDUs that are protected using the results of an EAP exchange.~~In other words,~~ MKA instances that transmit MKPDUs with different values of the Algorithm Agility parameter could use a different KDF (see 6.2.1) to derive the ICK (9.3.3), could specify the computation of the ICV in a different way, and could specify a different way for the participants in an EAP exchange to agree on a CAK (6.2.2). The flexibility provided allows a wide range of future challenges to be addressed, but the need for substantial analysis of any proposed alternate to the provisions of this standard in these areas means that no claim of conformance is facilitated currently for any such alternate. A future revision of this standard could provide such a claim, if needed to address cryptographic developments.

MKA's Algorithm Agility parameter does not identify the KDF used to derive the KEK, or the Key Wrap (see 6.2). ~~That identification is provided~~ They are identified by the MKA parameter set type used to encode the Key Wrap. MKA parameter sets 4 and 5 (Figure 11-11, Figure 11-12, Figure 11-13) use a particular KDF (6.2.1, 9.3.3) and Key Wrap (AES Key Wrap, 9.8.2, 9.12.1) by definition. A different Key Wrap, or a Key Wrap using a differently derived KEK, could be introduced by defining a further parameter set type while still allowing MKA participants to communicate by using MKPDUs with a familiar Algorithm Agility parameter value—thus allowing negotiation or fallback to known parameter set types.

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

7. Port-based network access control applications

7.7.2 System configuration and operation

Change the note to Figure 7-16 as follows:

NOTE—Figure 7-16 is based on Figure 15-1 of IEEE Std 802.1Q ~~(as amended by IEEE Std 802.1ad)~~.

Change the last sentence of the second paragraph of 7.7.2 as follows:

The interface stack shown includes the service access priority selection function described in 6.9 of IEEE Std 802.1Q ~~(as amended by IEEE Std 802.1ad)~~.

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

9. MACsec Key Agreement protocol (MKA)

Insert the following item(s) at the end of the list introduced by "This clause specifies …"

o) Management of the KaY and MKA (9.16).
p) Temporary suspension of MKA operation to facilitate in-service control plane software upgrades without disrupting existing secure connectivity (9.18).

Change the dashed list in the introductory text of Clause 9 as follows:

The following terms are used to identify roles within the protocol or protocol scenarios:

— **participant:** The personification of a single KaY's participation in a given MKA instance (i.e., transmitting and receiving MKPDUs protected by keys derived from a single given CAK and identified by a given CKN), operating with positive intent, and obeying the protocol.
— **actor:** The participant under discussion, usually in the KaY being described.
— **partners:** Other participants in the same MKA instance, and attached to the same LAN, as the actor.
— **successful actor:** An actor that has one or more live partners and is participating in an MKA instance that has elected a Key Server.
— **principal actor:** The successful actor selected by a KaY to control its associated PAC or SecY. ~~that is participating in the MKA instance with the highest priority Key Server.~~
— **member**: ~~A participant using MKA to establish Controlled Port connectivity with other participants.~~ The personification of a single KaY's participation in all MKA instances and use of other controls that determine the connectivity provided by its associated Controlled Port. A system is described as being member of a CA if it includes a Controlled Port providing connectivity using that CA.

9.1 Protocol design requirements

Insert an additional note after bullet c) as follows:

c) Following any period of 8 seconds during which all frames transmitted by each of a set of participants are delivered, once and without misordering, to each of the other participants, and the load imposed by frames received from an attacker does not exceed the resources of any participant, MKA will provide the keys and information required by each of its participants' clients, irrespective of the prior state of each participant or frames buffered by the LAN.

NOTE 1—The requirement is that of correctness: the protocol convergence time is bounded; rather than a performance goal. The figure of 8 seconds arises from the possibility that prior participants are being timed out (over a period of MKA Life Time, 6 seconds, see Table 9-3) just as a new participant joins, plus MKA Hello Time (2 seconds) to ensure that all participants have subsequently transmitted.

NOTE 2—If MKA operation is suspended (9.18), and the participants do not already possess the necessary keys and information, convergence will be delayed until MKA operation resumes.

Change the note following bullet k) as follows:

k) It allows its participants to ensure that the data frames protected by MACsec are not being delayed by more than 2 seconds.

NOTE ~~2~~3—Delay protection guards against an attack on the configuration protocols that MACsec is designed to protect by alternately delaying and delivering their PDUs. Delay protection does not operate if and when MKA operation is suspended (9.18).

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

Insert the following new text after the existing text of 9.1:

When the option to support MACsec Cipher Suites that use Extended Packet Numbering is implemented, MKA meets the following requirements:

m) Recovery, if lost, of the 32 most significant bits of the XPN, in support of the protocol correctness requirement c) above.

9.3.3 Derived keys

Change the text of 9.3.3, moving the fourth paragraph to become the second, and reversing the order of the present second and third paragraphs, so the entire text of the subclause (showing changes made to each paragraph) is as follows:

Each of the keys used by MKA is derived from the CAK ~~using the AES Cipher in CMAC mode (NIST Special Publication 800-38B)~~. The CAK is not used directly. The derived keys are tied to the identity of the CAK, and thus restricted to use with that particular CAK. ~~The KDF specified in 6.2.1 is used to derive these keys. The hexadecimal representations of each of the text strings used with this KDF is given in H.~~

To accommodate future developments in cryptography, each MKPDU conveys an Algorithm Agility parameter that identifies how the ~~KEK and~~ ICK ~~are~~ is derived from the CAK~~,~~ and how it is ~~these keys are~~ used. Each Algorithm Agility parameter value comprises four octets, the first three being those of an OUI (Organizationally Unique Identifier) allocated by the IEEE Registration Authority, and the fourth allocated by the organization to which that OUI has been allocated. The derivation of the ~~KEK and~~ ICK, and the use ~~and size~~ of ~~these~~ this key~~s~~ as specified in this standard, is identified by the value specified in Table 9-1.

The ICK is derived from the CAK using the KDF specified in 6.2.1. This KDF uses the AES Cipher in CMAC mode (IETF RFC 4493). The ICK is derived from the CAK using the following transform:

ICK = KDF(Key, Label, Keyid, ICKLength)

where

Key = CAK

Label = “IEEE8021 ICK”

Keyid = the first 16 octets of the CKN, with null octets appended to pad to 16 octets if necessary

ICKLength = two octets representing an integer value (128 for a 128 bit ICK, 256 for a 256 bit ICK) with the most significant octet first

~~In each case t~~The Label is a UTF-8 string, without a null or other termination, exactly 12 bytes in length (the quotes shown do not form part of the string and exactly one space separates ‘8021’ ~~and ‘KEK’, and ‘8021’~~ and ‘ICK’). The length of the Label is chosen to make the input to the PRF within the KDF exactly 32 bytes. The hexadecimal representations of each of the text strings used with this KDF and test vectors are given in Annex H.

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

To accommodate future developments in cryptography, each of the MKA parameter set types used by MKA to communicate a wrapped key identifies the Key Wrap Algorithm and KEK derivation (6.2.4, Figure 11-11, Figure 11-12, Figure 11-13) used. The KEK used by all parameter set types currently specified in this standard is derived from the CAK using the KDF specified in 6.2.1. This KDF uses the AES Cipher in CMAC mode (IETF RFC 4493). The KEK is derived from the CAK using the following transform:

KEK = KDF(Key, Label, Keyid, KEKLength)

where

Key = CAK
Label = "IEEE8021 KEK"
Keyid = the first 16 octets of the CKN, with null octets appended to pad to 16 octets if necessary
KEKLength = two octets representing an integer value (128 for a 128 bit KEK, 256 for a 256 bit KEK) with the most significant octet first

~~In each case t~~The Label is a UTF-8 string, without a null or other termination, exactly 12 bytes in length (the quotes shown do not form part of the string and exactly one space separates '8021' and 'KEK'~~, and '8021' and 'ICK'~~). The length of the Label is chosen to make the input to the PRF within the KDF exactly 32 bytes.

When SAKs and CAKs are distributed they are protected by the KEK, using an AES Key Wrap as defined in 9.8.2 and 9.12.1. ~~The number of bits in each SAK, and its use, is not tied to the value of MKA's Algorithm Agility parameter but is identified by the value of the MACsec Cipher Suite parameter.~~

SAKs should be derived from the CAK as specified in 9.8.1, but may also be generated directly by the Key Server's strong random number generator (RNG, 9.2.1). Distributed CAKs, when used, shall be random values generated by the MKA Key Server RNG. Each distributed CAK is distinct from previously distributed CAKs, so that an MKA participant or attacker holding only the current CAK cannot determine a previously distributed CAK. This allows implementation of a policy of perfect forward security, with a fresh CAK being distributed when each participant joins a CA, so that participant cannot decrypt wrapped keys from previously transmitted MKA frames.

NOTE—MKA does not require fresh CAK distribution when a new participant joins a CA, as that would prolong the process of joining.

Change Table 9-1 (correcting it to match the approval date and designation of IEEE Std 802.1X-2010, as identified in the text of 9.3.3 as "this standard") as follows:

Table 9-1—MKA Algorithm Agility parameter values

Parameter value	Specification
00-80-C2-01	IEEE Std 802.1X-20~~09~~10

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

9.4.3 Determining liveness

Change the text and notes of 9.4.3 as follows:

A participant proves liveness to each of its peers by including their MI, together with an acceptably recent MN, in an MKPDU with the participant's own MI and MN.

To avoid a new participant having to respond to each MKPDU from each partner as it is received, or trying to delay its reply until it is likely that MI.MN tuples have been received from all potential partners, each participant maintains and advertises both a Live Peer~~s~~ List and a Potential Peer~~s~~ List. The Live Peer~~s~~ List includes all the peers that have included the participant's MI and a recent MN in a recent MKPDU, and the Potential Peer~~s~~ List includes all the other peers that have transmitted an MKPDU that has been directly received by the participant or that were included in the Live Peer~~s~~ List of an MKPDU transmitted by a peer that has proved liveness. Peers are removed from each list when an interval of between MKA Life Time (see Table 9-3) and MKA Life Time plus MKA Hello Time has elapsed since the participant's recent MN (see above) was transmitted. This time is sufficient to ensure that two or more MKPDUs will have been lost or delayed prior to the incorrect removal of a live peer.

NOTE 1—The specified use of the Live and Potential Peer Lists thus permits rapid removal of participants that are no longer active or attached to the LAN while reducing the number of MKPDUs transmitted during group formation. For example, a new participant will be admitted to an established group after receiving, then transmitting, one MKPDU.

NOTE 2—A suspended participant (9.18) will be removed from the Live and Potential Peer Lists as described, but its associated SecY will still be able to transmit and receive secure frames until other CA members adopt a new SAK.

Insert a new subclause 9.4.6 as follows:

9.4.6 Active and passive participants

A participant can be active, transmitting periodic MKPDUs, or passive. A passive participant will become active for a period of MKA Lifetime following the receipt of an MKPDU from a feasible partner, i.e., provided that either the receiving participant or the partner is prepared to act as a Key Server. Whether a participant is to be active when first created, and whether it is to remain active in the absence of feasible partners depends on the port-based network access control application. The creation of passive participants supports systems that have many potential peers, with only one or a few likely to be connected at a time. Participants that are always active are desirable where connectivity is provided by media that do not reliably signal loss and resumption of connectivity, as can be the case for infrastructure links supported by virtual media. If all the participants in a potential CA can be passive, and an extended and undetected network outage occurs, it is possible that the potential CA members will fail to transmit MKPDUs, resulting in a permanent lack of connectivity.

NOTE 1—The condition of having recently received an MKPDU from a feasible partner can be determined by inspecting the participant's Live Peer List and Potential Peer List.

NOTE 2—The model of Logon Process operation encompasses participant creation, deletion, and control of active or passive participation (12.2, 12.5.2). The CAK cache provides management (see activate in 9.16).

An active participant will remain active, even in the absence of received MKPDUs, while a suspension is in progress (provided that the participant is not itself suspended). A suspended participant will resume active operation if and only if

a) Its CAK was previously cached, and
b) The management controls associated with that cached CAK specify that it is to be active on resumption (9.16).

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

9.5 Key server election

Change the list in 9.5 as follows:

The participants in a given MKA instance agree on a Key Server, responsible for the following:

a) Deciding on the use of MACsec (9.6)
b) Cipher suite selection (9.7)
c) SAK generation and distribution (9.8)
d) SA assignment (9.10.1)
e) Identifying the CA when two or more CAs merge (9.15)
f) CA formation and group CAK distribution (9.15)
g) Initiating, continuing, and terminating MKA suspension (9.18)

If the CAK is a pairwise CAK derived directly from EAP (see 6.2.2), the MKA participant for the PAE that was the EAP Authenticator will be the Key Server, and will not accept information [a) through ~~f~~g) above] from any other participant that attempts to act as the Key Server for that MKA instance.

Change the fourth paragraph of 9.5 as follows:

If a KaY participates in multiple MKA instances so that there are several actors—one per instance—for a given port, then only the actor selected as the principal actor (12.1) will (if elected Key Server for its CAK) distribute SAKs ~~and perform other Key Server functions. An actor that has been elected a Key Server by its peers but is not the principal actor for its KaY (12.1) will, by not choosing and distributing the parameters necessary for communication to its peers, ensure that a single principal actor is chosen for all the MKA Entities that participate in overlapping CAK, CKN distribution on a LAN, and that a single unambiguous MACsec CA can be formed on that LAN.~~ Since the factors that cause a principal actor to be selected from its peers are the same for different CAK, CKN tuples with the same distribution, replacement of a principal actor by its successor will occur, whenever possible, without a change of Key Server. This succession plan ensures that the SAKs distributed using one CAK, CKN tuple can be followed immediately by SAKs distributed by a successor CAK, CKN without any loss of MACsec connectivity. To minimize the chance of a CA member that possesses both CAKs temporarily losing connectivity, a Key Server should not distribute an SAK using the new CAK until MKA Life Time (Table 9-3) has elapsed after it has started participating with that CAK, and should not delete the participant for the prior CAK until MKA Life Time has elapsed after that new SAK is first distributed. The CP state machine (Figure 12-2) ensures that a new SAK is not distributed until the Key Server is receiving and transmitting using a single SAK.

Delete the current note and insert two new notes as follows:

~~NOTE—Choice of the principal actor by each KaY to receive information from, or to act as, the Key Server ensures that two PAEs will choose the same Key Server even if they both comprise EAP Authenticator and Supplicant functionality, and each has authenticated as the Authenticator. The KaY with the highest priority will be the Key Server.~~

NOTE 1—If two PAEs are each capable of acting as both an EAP Authenticator and an EAP Supplicant, their interaction can result in two instances of successful mutual authentication with each acting as the Authenticator in one. Thus two MKA instances can be created, and each PAE's KaY will be elected Key Server for one instance. However, each KaY will select, as its principal actor, its participant in the MKA instance with the highest priority Key Server. That Key Server can then use that MKA instance to distribute SAKs (or select unauthenticated connectivity, see 12.3), and the participants in the other MKA instance can be deleted.

NOTE 2—A number of KaYs participating in multiple MKA instances will still succeed in configuring a single CA even if each participates in a different subset of those instances, provided that the highest priority Key Server in each subset itself participates in an MKA instance with a higher priority Key Server or is the highest priority Key Server. For example, assume KaYs A, B, C, D (say) in decreasing priority order, with two MKA instances with participants {A, B, C} and {B, D} respectively. Although B will be elected Key Server for the {B, D} instance, it will not distribute SAKs to D, as B's principal actor will be in {A, B, C}. Thus a single CA will be created, including the ports associated with A,

Copyright © 2014 IEEE. All rights reserved.
Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Documents
Document Sharing Hub

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1

B, and C, but excluding D's. However, scenarios of this type are most likely to result from errors in manual key distribution. They can give rise to temporary interruptions or unwanted connectivity, particularly where in-service upgrades are to be performed and need to be eliminated as part of managing upgrades (9.18.6).

9.6.1 MKPDU application data

Change 9.6.1 as follows:

Each MKA participant encodes the following information in every MKPDU transmitted:

a) MACsec capability, indicating whether MACsec is implemented, and if so whether the implementation provides integrity protection only, integrity and integrity with confidentiality, or integrity and integrity with confidentiality with a selectable confidentiality offset of 0, 30, or 50 octets (see Table 11-6, IEEE Std 802.1AE-2006).

NOTE—IEEE Std 802.1AE-2006 introduced the confidentiality offset to facilitate early MACsec deployment on existing systems that needed to store received frames before applying MACsec processing and that needed to examine the initial octets of received frames to decide where to store those frames. The XPN Cipher Suites standardized in IEEE Std 802.1AEbw-2013 do not support confidentiality offsets of other than 0.

b) MACsec desired, a flag, set if the participant desires the use of MACsec to protect frames.

9.7.1 MKPDU application data

Change 9.7.1 as follows:

A participant that believes itself to be the Key Server and its KaY's principal actor encodes the following information with each MACsec SAK that it distributes, unless the mandatory Default Cipher Suite GCM-AES-128 is to be used:

a) MACsec Cipher Suite, the Cipher Suite reference number.

The following information is also distributed with each MACsec SAK:

b) Confidentiality Offset, indicating whether confidentiality is to be provided, and whether an offset of 0, 30, or 50 octets is used (see IEEE Std 802.1AE-2006).

If a receiving MKA participant does not implement the referenced Cipher Suite with the selected confidentiality offset, the distributed SAK will not be installed (12.4). An MKA participant should advertise any Cipher Suites implemented in addition to the Default Cipher Suite by including an Announcement parameter set (11.11.1 Figure 11-15) with a MACsec Cipher Suites TLV (11.12.3) in each MKPDU transmitted.

NOTE— ~~This standard does not currently provide any way for MKA to negotiate the use of an alternative cipher suite or a confidentiality offset. While the format of an MKPDU (Clause 11) can accommodate the definition of additional parameter sets, this standard deliberately does not provide a way to add non-standard parameters.~~ The XPN Cipher Suites standardized in IEEE Std 802.1AEbw-2013 do not support confidentiality offsets of other than 0.

Documents Document Sharing Hub

Copyright © 2014 IEEE. All rights reserved.

Authorized licensed use limited to: Tsinghua University. Downloaded on February 27,2026 at 11:26:46 UTC from IEEE Xplore. Restrictions apply.

Full document details: ISO/IEC/IEEE 8802-1X:2013/Amd. 1