

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 3:
Ethernet Data Encryption devices

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.1AEcg™-2017
(Amendment to
IEEE Std 802.1AE™-2006
as amended by
IEEE Std 802.1AEbn™-2011
and IEEE Std 802.1AEbw™-2013)

IEEE Std 802.1AEcg™-2017

(Amendment to
IEEE Std 802.1AE™-2006
as amended by
IEEE Std 802.1AEbn™-2011
and IEEE Std 802.1AEbw™-2013)

**IEEE Standard for
Local and metropolitan area networks—**

Media Access Control (MAC) Security

**Amendment 3:
Ethernet Data Encryption devices**

Sponsor

**LAN/MAN Standards Committee
of the
IEEE Computer Society**

Approved 14 February 2017
IEEE-SA Standards Board

Abstract: Ethernet Data Encryption devices (EDEs) are specified in this amendment. An EDE is a two-port bridge that uses MACsec to provide secure connectivity for attached customer bridges, or for attached provider bridges. EDEs may allow the customer (or provider) bridges to continue to use a VLAN Identifier (VID) in transmitted frames to select (as already specified in IEEE Std 802.1Q™) between provider network or provider backbone network services.

Keywords: amendment, authorized port, confidentiality, data origin authenticity, EDE, Ethernet Data Encryption device, IEEE 802.1AE, IEEE 802.1AEcg, 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 © 2017 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 19 May 2017. 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 978-1-5044-3725-7 STD22415
Print: ISBN 978-1-5044-3726-4 STDPD22415

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 subsequent 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 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/browse/standards/collection/ieee> 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 holder 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 802.1 working group had the following membership:

Glenn Parsons, *Chair*

John Messenger, *Vice Chair*

Mick Seaman, *Security Task Group Chair, Editor*

Seo Young Baek	Marc Holness	Karen Randall
Shenghua Bao	Lu Huang	Maximilian Riegel
Jens Bierschenk	Tony Jeffree	Dan Romascanu
Steinar Bjornstad	Michael Johas Teener	Jessy V. Rouyer
Christian Boiger	Hal Keen	Eero Ryytty
Paul Bottorff	Stephan Kehrer	Soheil Samii
David Chen	Philippe Klein	Behcet Sarikaya
Feng Chen	Jouni Korhonen	Frank Schew
Weiyang Cheng	Yizhou Li	Johannes Sp
Rodney Cummings	Christophe Mangin	Wilfried Steiner
János Farkas	Tom McBeath	Patricia Thaler
Norman Finn	James McIntosh	Paul Uebber
Geoffrey Garner	Tero Mustala	Paul Uebber
Eric W. Gray	Hiroki Nakano	Ha Wang
Craig Gunther	Bob Noseworthy	Karl Weber
Marina Gutierrez	Donald R. Pannell	Brian Weis
Stephen Haddock	Walter Pieniac	Ardon Woods
Mark Hantel	Michael Potts	Andreas Zein
Patrick Heffernan		Helge Zinner
		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	Noriyuki Ikeu	Karen Randall
Richard Alfvén	Osamu Ishida	Alon Regev
Johann Amsenga	Atsushi Ito	Maximilian Riegel
Butch Anton	Rajiv Joshi	Robert Robinson
Nancy Bravin	Seungwon Jeong	Jessy Rouyer
William Byrd	Piotr Karocki	Richard Roy
Juan Carreon	J. Matt Kent	Mick Seaman
Keith Chow	Stuart Kerry	Thomas Starai
Charles Cook	Yongbum Kim	Walter Struppler
Rodney Cummings	Hyeong Ho Lee	Patricia Thaler
Janos Farkas	James Lepp	Thomas Tullia
Matthias Fritsche	Jon Lewis	Mark-Rene Uchida
Yukihiro Fujimoto	Elvis Maculuba	Prabodh Varshney
Joel Goergen	Michael McInnis	George Vlantis
Randall Groves	Michael Montemurro	Khurram Waheed
Joseph Gymer	Michael Newman	Hung-Yu Wei
Stephen Haddock	Satoshi Obara	Andreas Wolf
Marc Hernandez	Bansi Patel	Chun Yu Charles Wong
Werner Hoelzl	Arumugam Paventhan	Oren Yuen
		Zhen Zhou

When the IEEE-SA Standards Board approved this standard on 14 February 2017, it had the following membership:

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

Chuck Adams
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Gary Hoffman

Michael Janezic
Thomas Koshy
Joseph L. Koepfinger1
Kevin Lu
Daleep Mohla
Damir Novosel
Ronald C. Petersen
Annette D. Reilly

Robby Robson
Dorothy Stanley
Adrian Stephens
Mehmet Ulema
Phil Wennblom
Howard Wolfman
Yu Yuan

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.1AEcg-2017, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security—Amendment 3: Ethernet Data Encryption devices.

The first edition of IEEE Std 802.1AE™ was published in 2006. A first amendment, IEEE Std 802.1AEbn™-2011, added the option of using the GCM-AES-256 Cipher Suite. A second, IEEE Std 802.1AEbw™-2013 added the GCM-AES-XPN-128 and GCM-AES-XPN-256 Cipher Suites. These extended packet numbering Cipher Suites allow more than 2^{32} frames to be protected with a single Secure Association Key (SAK) and so ease the timeliness requirements on key agreement protocols for very high-speed (100 Gb/s plus) operation. This third amendment, IEEE Std 802.1AEcg™-2017, specifies Ethernet Data Encryption devices (EDEs).

Relationship between IEEE Std 802.1AE and other IEEE Std 802 standards

IEEE Std 802.1X™-2010 specifies Port-based Network Access Control, and provides a means of authenticating and authorizing devices attached to a LAN, and includes the MACsec Key Agreement protocol (MKA) necessary to make use of IEEE 802.1AE.

IEEE Std 802.1AE is not intended for use with IEEE Std 802.11™ Wireless LAN Medium Access Control. An amendment to that standard, IEEE Std 802.11i™-2004, also makes use of IEEE Std 802.1X™, thus facilitating the use of a common authentication and authorization framework for LAN media to which this standard applies and for Wireless LANs.

Contents

1.	Overview.....	15
1.2	Scope.....	15
2.	Normative references.....	16
3.	Definitions.....	18
4.	Abbreviations and acronyms.....	20
5.	Conformance.....	21
5.1	Requirements terminology.....	21
5.2	Protocol Implementation Conformance Statement (PICS).....	22
5.3	Required capabilitiesMAC Security Entity requirements.....	22
5.4	Optional capabilitiesMAC Security Entity options.....	23
5.5	EDE conformance.....	24
5.6	EDE-M conformance.....	24
5.7	EDE-CS conformance.....	25
5.8	EDE-CC conformance.....	25
5.9	EDE-SS conformance.....	25
6.	Secure provision of the MAC Service.....	26
6.1	MAC Service primitives and parameters.....	26
6.2	MAC Service connectivity.....	26
6.4	MAC status parameters.....	27
6.5	MAC point-to-point parameters.....	27
6.10	Quality of service maintenance.....	27
7.	Principles of secure network operation.....	29
7.1	Support of the secure MAC Service by an individual LAN.....	29
7.3	Use of the secure MAC Service.....	30
8.	MAC Security Protocol (MACsec).....	32
8.3	MACsec operation.....	32
9.	Encoding of MACsec protocol data units.....	34
9.9	Secure Channel Identifier (SCI).....	34
10.	Principles of MAC Security Entity (SecY) operation.....	35
10.1	SecY overview.....	35
10.2	SecY functions.....	35
10.4	SecY architecture.....	36
10.5	Secure frame generation.....	36
10.6	Secure frame verification.....	40
10.7	SecY management.....	41
11.	MAC Security in Systems.....	52
11.1	MAC Service interface stacks.....	52

11.3	MACsec in MAC Bridges.....	52
11.4	MACsec in VLAN-aware Bridges.....	53
11.8	MACsec and multi-access LANs.....	53
13.	Management protocol MAC Security Entity MIB	55
13.1	Introduction.....	55
13.4	Security considerations	55
13.5	Structure of the MIB module	56
13.6	Definitions for MAC Security Entity (SecY) MIB definitions.....	62
14.	Encoding of MACsec protocol data units.....	100
14.5	Default Cipher Suite (GCM–AES–128).....	100
14.6	GCM-AES-256	100
15.	Ethernet Data Encryption devices.....	101
15.1	EDE characteristics.....	101
15.2	Securing LANs with EDE-Ms	102
15.3	Securing connectivity across PBNs	104
15.4	Securing PBN connectivity with an EDE-M.....	105
15.5	Securing PBN connectivity with an EDE-CS	106
15.6	Securing PBN connectivity with an EDE-CC	108
15.7	Securing PBN connectivity with an EDE-SS	111
15.8	EDE Interoperability.....	111
15.9	EDEs, CFM, and UNI Access	113
16.	Using MIB modules to manage EDEs	114
16.1	Security considerations	114
16.2	EDE-M Management.....	114
16.3	EDE-CS Management.....	114
16.4	EDE-CC and EDE-SS Management.....	114
Annex A (normative) PICS Proforma.....		116
A.5	Major capabilities	116
A.9	Secure Frame Verification.....	118
A.12	Additional fully conformant Cipher Suite capabilities	122
A.13	Additional variant Cipher Suite capabilities.....	123
Annex B (informative) Bibliography		125
Annex D (normative) PICS Proforma for an Ethernet Data Encryption device.....		127
D.1	Introduction.....	127
D.2	Abbreviations and special symbols.....	127
D.3	Instructions for completing the PICS proforma.....	128
D.4	PICS proforma for IEEE Std 802.1AE EDE	130
D.5	EDE type and common requirements	131
D.6	EDE-M Configuration	132
D.7	EDE-CS Configuration	132
D.8	EDE-CC Configuration.....	133
D.9	EDE-SS Configuration	133

Annex E (informative)	MKA operation for multiple transmit SCs	134
Annex F (informative)	EDE Interoperability and PAE addresses	136
Annex G (informative)	Management and MIB revisions.....	139
G.1	Counter changes.....	140
G.2	Available Cipher Suites.....	141

Figures

Figure 7-7	Secure Channel and Secure Association Identifiers	30
Figure 10-4	Management controls and counters for secure frame generation	36
Figure 10-5	Management controls and counters for secure frame verification	38
Figure 10-6	SecY managed objects	43
Figure 11-4	MACsec in an IEEE 802.1D VLAN-unaware MAC Bridge	52
Figure 11-5	IEEE 802.1D VLAN-unaware MAC Bridge Port with MACsec	53
Figure 11-6	Addition of MAC Security to a VLAN-aware MAC Bridge	53
Figure 11-15	An example multi-access LAN	54
Figure 13-1	Secy MIB structure	57
Figure 15-1	EDE-Ms connected by a point-to-point LAN	102
Figure 15-2	EDE-Ms securing a point-to-point LAN between Provider Bridges	103
Figure 15-3	MACsec protected frame traversing a PBN	104
Figure 15-4	EDE-Ms securing point-to-point LAN connectivity across a PBN	105
Figure 15-5	EDE-Ms securing multi-point PBN connectivity	106
Figure 15-6	Example of a network with an EDE-CS	107
Figure 15-7	EDE-CS connected to a PBN S-tagged interface	108
Figure 15-8	Using an EDE-CC with a C-tagged provider service interface	109
Figure 15-9	EDE-CC architecture	110

Tables

Table 10-1	Management controls and SecTAG encoding	39
Table 13-1	Controlled Port service management.....	59
Table 13-2	Transmit and receive SC management	60
Table 13-3	Transmit and receive statistics	61
Table 13-4	Cipher Suite information	62
Table 15-1	PAE Group Addresses	111
Table 15-2	PAE Group Address use	112
Table F-1	Interoperability scenarios and PAE Addresses	138

IEEE Standard for Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 3: Ethernet Data Encryption devices

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.