

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

Media Access Control (MAC) Security

**Amendment 1: Galois Counter Mode—
Advanced Encryption Standard—
256 (GCM-AES-256) Cipher Suite**

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.1AEbn™-2011
(Amendment to
IEEE Std 802.1AE™-2006)

14 October 2011

IEEE Std 802.1AEbn™-2011

(Amendment to
IEEE Std 802.1AE™-2006)

**IEEE Standard for
Local and metropolitan area networks—
Media Access Control (MAC) Security
Amendment 1: Galois Counter Mode—
Advanced Encryption Standard—
256 (GCM-AES-256) Cipher Suite**

Sponsor

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

Approved 10 September 2011

IEEE-SA Standards Board

Abstract: This amendment specifies the GCM-AES-256 Cipher Suite as an option in addition to the existing mandatory to implement Default Cipher Suite, GCM-AES-128.

Keywords: authenticity, authorized port, confidentiality, data origin integrity, IEEE 802.1AEbn, 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 © 2011 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 14 October 2011. 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 978-0-7381-6735-0 STD97152
Print: ISBN 978-0-7381-6736-7 STDPD97152

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.

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 or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied “**AS IS.**”

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. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, 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 publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received 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 interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the 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, explanation, or interpretation of the IEEE. Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required.

Comments and recommendations on standards, and requests for interpretations should be addressed to:

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

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, 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.

Introduction

This introduction is not part of IEEE Std 802.1AEbn-2011, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security—Amendment 1: Galois Counter Mode—Advanced Encryption Standard—256 (GCM-AES-256) Cipher Suite.

The first edition of IEEE Std 802.1AE was published in 2006. This first amendment to that standard adds the option of using the GCM-AES-256 Cipher Suite.

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.

This standard 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.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard 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

This document is copyrighted by the IEEE. It is made available 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 this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards 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. 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 Standards Association website at <http://ieeexplore.ieee.org/xpl/standards.jsp>, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE 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.

Interpretations

Current interpretations can be accessed at the following URL: <http://standards.ieee.org/findstds/interps/index.html>.

Patents

Attention is called to the possibility that implementation of this amendment may require use of subject matter covered by patent rights. By publication of this amendment, no position is taken with respect to the existence or validity of any patent rights in connection therewith. 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 amendment 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 submitted to the IEEE-SA for approval, the IEEE P802.1 Working Group had the following membership:

Tony Jeffree, *Chair*
Paul Congdon, *Vice Chair*
Mick Seaman, *Editor and Chair, Security Task Group*

Zehavit Alon	Eric Gray	Eric Multanen
Yafan An	Yingjie Gu	David Olsen
Ting Ao	Craig Gunther	Donald Pannell
Peter Ashwood-Smith	Michael Johas Teener	Glenn Parsons
Christian Boiger	Stephen Haddock	Mark Pearson
Paul Bottorff	Hitoshi Hayakawa	Joseph Pelissier
Rudolf Brandner	Hal Keen	Rene Raeber
Craig Carlson	Srikanth Keesara	Karen T. Randall
Rodney Cummings	Yongbum Kim	Josef Roese
Claudio Desanti	Philippe Klein	Dan Romascanu
Zheming Ding	Oliver Kleineberg	Jessy Rouyer
Donald Eastlake, III	Michael Krause	Ali Sajassi
Janos Farkas	Lin Li	Panagiotis Saltsidis
Donald Fedyk	Jeff Lynch	Rakesh Sharma
Norman Finn	Ben Mack-Crane	Kevin Stanton
Ilango Ganga	David Martin	Robert Sultan
Geoffrey Garner	John Messenger	Patricia Thaler
Anoop Ghanwani	John Morris	Chait Tumuluri
Mark Gravel		Maarten Visser

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

Thomas Alexander	Atsushi Ito	Robert Robinson
Butch Anton	Raj Jain	Benjamin Rolfe
Nancy Bravin	Junghoon Jee	Jessy Rouyer
William Byrd	Tony Jeffree	Herbert Ruck
Radhakrishna Canchi	Michael Johas Teener	Randall Safier
Keith Chow	Shinkyō Kaku	Joseph Salowey
Charles Cook	Piotr Karocki	Raymond Savarda
Claudio DeSanti	Stuart J. Kerry	Bartien Sayogo
Wael Diab	Lior Khermosh	Mick Seaman
Patrick Diamond	Yongbum Kim	Shusaku Shimada
Thomas Dineen	Geoff Ladwig	Kapil Sood
Sourav Dutta	Paul Lambert	Thomas Starai
Donald Fedyk	William Lumpkins	Walter Struppler
Yukihiro Fujimoto	Greg Luri	Joseph Tardo
Devon Gayle	Elvis Maculuba	Michael Johas Teener
Gregory Gillooly	Edward McCall	Patricia Thaler
Evan Gilman	Michael McInnis	Mark-Rene Uchida
Ron Greenthaler	Gary Michel	Dmitri Varsanofiev
Randall Groves	Michael S. Newman	Prabodh Varshney
C. Guy	Satoshi Obara	John Vergis
John Hawkins	Glenn Parsons	Hung-Yu Wei
David Hunter	Karen T. Randall	Brian Weis
Paul Isaacs	Maximilian Riegel	Ludwig Winkel
		Oren Yuen

When the IEEE-SA Standards Board approved this standard on 10 September 2011, it had the following membership:

Richard H. Hulett, *Chair*
John Kulick, *Vice Chair*
Robert M. Grow, *Past Chair*
Judith Gorman, *Secretary*

Masayuki Ariyoshi
William Bartley
Ted Burse
Clint Chaplin
Wael Diab
Jean-Philippe Faure
Alexander Gelman
Paul Houzé

Jim Hughes
Joseph L. Koepfinger*
David J. Law
Thomas Lee
Hung Ling
Oleg Logvinov
Ted Olsen

Gary Robinson
Jon Walter Rosdahl
Sam Sciacca
Mike Seavey
Curtis Siller
Phil Winston
Howard L. Wolfman
Don Wright

*Member Emeritus

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

Satish Aggarwal, NRC Representative
Richard DeBlasio, DOE Representative
Michael Janezic, NIST Representative

Catherine Berger
IEEE Project Editor

Patricia Gerdon
IEEE Standards Program Manager, Technical Program Development

Contents

1. Overview	2
1.1 Introduction	2
1.2 Scope	2
2. Normative references	3
6. Secure provision of the MAC Service	4
6.1 MACsec connectivity	4
7. Principles of secure network operation	5
8. MAC Security Protocol (MACsec)	6
9. Encoding of MACsec protocol data units	7
9.8 Transmit SA status	7
10. Principle of MAC Security Entity (SecY) operation	8
11. MAC Security in Systems	9
11.7 MACsec in Provider Bridged Networks	9
14. Cipher Suites	10
14.1 Cipher Suite use	10
14.4 Cipher Suite conformance	10
14.5 Default Cipher Suite (GCM-AES-128)	11
14.6 GCM-AES-256	11
Annex B (informative) Bibliography	13
Annex C (informative) MACsec Test Vectors	14
C.1 Integrity protection (54-octet frame)	15
C.2 Integrity protection (60-octet frame)	18
C.3 Integrity protection (65-octet frame)	21
C.4 Integrity protection (79-octet frame)	24
C.5 Confidentiality protection (54-octet frame)	27
C.6 Confidentiality protection (60-octet frame)	30
C.7 Confidentiality protection (61-octet frame)	33
C.8 Confidentiality protection (75-octet frame)	36

Figures

Figure 11-14 Provider network with priority selection and aggregation..... 9

Figure 14-1 Cipher Suite Protect and Validate operations 10

Tables

Table 14-1	MACsec Cipher Suites.....	10
Table C-1	Unprotected frame (example)	15
Table C-2	Integrity protected frame (example)	15
Table C-3	GCM-AES-128 Key and calculated ICV (example)	16
Table C-4	GCM-AES-256 Key and calculated ICV (example)	17
Table C-5	Unprotected frame (example)	18
Table C-6	Integrity protected frame (example)	18
Table C-7	GCM-AES-128 Key and calculated ICV (example)	19
Table C-8	GCM-AES-256 Key and calculated ICV (example)	20
Table C-9	Unprotected frame (example)	21
Table C-10	Integrity protected frame (example)	21
Table C-11	GCM-AES-128 Key and calculated ICV (example)	22
Table C-12	GCM-AES-256 Key and calculated ICV (example)	23
Table C-13	Unprotected frame (example)	24
Table C-14	Integrity protected frame (example)	24
Table C-15	GCM-AES-128 Key and calculated ICV (example)	25
Table C-16	GCM-AES-256 Key and calculated ICV (example)	26
Table C-17	Unprotected frame (example)	27
Table C-18	Confidentiality protected frame (example).....	27
Table C-19	GCM-AES-128 Key, Secure Data, and ICV (example)	28
Table C-20	GCM-AES-256 Key, Secure Data, and ICV (example)	29
Table C-21	Unprotected frame (example)	30
Table C-22	Confidentiality protected frame (example).....	30
Table C-23	GCM-AES-128 Key, Secure Data, and ICV (example)	31
Table C-24	GCM-AES-256 Key, Secure Data, and ICV (example)	32
Table C-25	Unprotected frame (example)	33
Table C-26	Confidentiality protected frame (example).....	33
Table C-27	GCM-AES-128 Key, Secure Data, and ICV (example)	34
Table C-28	GCM-AES-256 Key, Secure Data, and ICV (example)	35
Table C-29	Unprotected frame (example)	36
Table C-30	Confidentiality protected frame (example).....	36
Table C-31	GCM-AES-128 Key, Secure Data, and ICV (example)	37
Table C-32	GCM-AES-256 Key, Secure Data, and ICV (example)	38

IEEE Standard for Local and metropolitan area networks— Media Access Control (MAC) Security Amendment 1: Galois Counter Mode— Advanced Encryption Standard— 256 (GCM-AES-256) Cipher Suite

IMPORTANT NOTICE: *This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.*

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>.

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 ~~striketrough~~ (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.

1. Overview

1.1 Introduction

Change the fourth paragraph as follows:

To deliver these benefits, MACsec has to be used in conjunction with appropriate policies for higher-level protocol operation in networked systems, an authentication and authorization framework, and network management. IEEE Std 802.1X ~~P802.1afTM~~ [B2]¹ provides authentication and cryptographic key distribution.

1.2 Scope

Change bullet i) as follows:

- i) Specifies the interface/exchanges between a SecY and its associated and collocated MAC Security Key Agreement Entity (KaY, IEEE Std 802.1X ~~P802.1af~~ [B2]) that provides and updates cryptographic keys.

Change bullet o) as follows:

- o) Specify how the relationships between MACsec protocol peers are discovered and authenticated, as supported by key management or key distribution protocols, but makes use of IEEE Std 802.1X ~~P802.1af~~ Key Agreement for MAC security to achieve these functions.