IEEE SA
STANDARDS ASSOCIATION

STANDARDS

IEEE Standard for Low-Rate Wireless Networks

Amendment 3: Advanced Encryption Standard (AES)-256 Encryption and Security Extensions

IEEE Computer Society

Developed by the
LAN/MAN Standards Committee

IEEE Std 802.15.4y™-2021
(Amendment to IEEE Std 802.15.4™-2020
as amended by IEEE Std 802.15.4z™-2020
and IEEE Std 802.15.4w™-2020)

IEEE

IEEE Std 802.15.4y™-2021
(Amendment to IEEE Std 802.15.4™-2020
as amended by IEEE Std 802.15.4z™-2020
and IEEE Std 802.15.4w™-2020)

IEEE Standard for Low-Rate Wireless Networks

Amendment 3: Advanced Encryption Standard (AES)-256 Encryption and Security Extensions

Developed by the

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 9 May 2021

IEEE SA Standards Board

Abstract: This amendment defines security extensions to IEEE Std 802.15.4 adding AES-256-CCM plus a cipher suite/authentication method registry and a process for inclusion of additional algorithms. The registry defines a capability to align IEEE Std 802.15.4 with the security requirements of higher layer standards.

Keywords: AEAD, AES-128, AES-128-CCM, AES-256, AES-256-CCM, algorithm agility, authentication, ciphers, encryption, IEEE 802.15.4™, low data rate, low power, security, wireless personal area network, WPAN

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

PDF: ISBN 978-1-5044-7558-7 STD24693
Print: ISBN 978-1-5044-7559-4 STDPD24693

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

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

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system. An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the IEEE SA Patent Policy.

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this IEEE standard was completed, the IEEE 802.15 Working Group had the following membership:

Patrick W. Kinney, *Chair*
Rick Alfvin, *Vice Chair*
Philip E. Beecher, *Vice Chair*
Clint Powell, *Vice Chair, Secretary*
James P. K. Gilb, *Technical Editor*
Benjamin A. Rolfe*, Treasurer*

Don Sturek, *Task Group 4y Chair and Technical Editor*
Peter Yee, *Task Group 4y Vice Chair*

Koorosh Akhavan
David Barras
Tuncer Baykas
Harry Bims
Lennert Bober
Chris Calvert
Clint Chaplin
Sangsung Choi
Nathan Clanney
Michael G. Cotton
Boris Danev
Hendricus De Ruijter
Guido Dolmans
Igor Dotlic
Ersen Ekrem
Robert Finch
Kiyoshi Fukui
Michael Gagne
Tim Godfrey
Jianlin Guo
Takamitsu Hafuka
Joachim Hammerschmidt
Shinsuke Hara
Hiroshi Harada
Jerome Henry
Christopher Hett
Roger Hislop
Jay Holcomb
Oliver Holland
Iwao Hosako
Tetsushi Ikegami
Yeong Min Jang
Jeng-Shiann Jiang
Seong-Soon Joo
Volker Jungnickel
Juha Juntunen
Yoshio Kashiwagi
Shoichi Kitazawa
Tero Kivinen
Ryuji Kohno
Fumihide Kojima
Ann Krieger
Thomas Kuerner
Takashi Kuramochi
Hideyuki Kuribayashi
Mingyu Lee
Frank Leong
Huan-Bang Li
Sang-Kyu Lim
Xiliang Luo
Masood Maqbool
Yuki Matsumura
Gianfranco Miele
Apurva Mody
Ayman Naguib
Seiji Nakanishi
Kathleen Nelson
Jaroslaw Niewczas
Paul Nikolich
Ryota Okumura
Philip Orlik
Clark Palmer
Glenn Parsons
Riku Pirhonen
Joe Polland
Ivan Reede
Joerg Robert
Alessandra Rocha
Ruben E. Salazar Cardozo
Stephan Sand
Eren Sasoglu
Nikola Serafimovski
Daoud Serang
Kunal Shah
Tushar Shah
Menashe Shahar
Stephen Shellhammer
Guy Simpson
Frederick Smith
William Smith
Gary Stuebing
Hitoshi Tanaka
Craig Tedrow
Hiroyuki Toda
Billy Verso
Johannes Wechsler
Shang-Te Yang
Sven Zeisberg

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

Philip E. Beecher
Abdoulaye Berthe
Steven Bezner
Riccardo Brama
Jon Brasher
Vern Brethour
William Byrd
Paul Cardinal
Juan Carreon
Pin Chang
Suresh Channarasappa
Hendricus De Ruijter
Liu Fangfang
Avraham Freedman
Dan Friedman
David Fuschi
Jalal Gohari
Mark Henley
Marco Hernandez
Shui Heung
Werner Hoelzl
Klaus Hueske
Richard Jessop
Piotr Karocki

Stuart Kerry
Evgeny Khorov
Yongbum Kim
Shoichi Kitazawa
Tero Kivinen
Yasushi Kudoh
Susan Land
Hyeong Ho Lee
Juan Antonio Lloret Egea
Dennis Neitzel
Satoshi Oyama
Bansi Patel
Arumugam Paventhan
Clint Powell
Pon Ramachandra Moorthy Ramasamy
R. K. Rannow
James Reilly
Maximilian Riegel
Joerg Robert
Robert Robinson
Benjamin A. Rolfe
Naotaka Sato
Kunal Shah
Gary Stuebing
Gerald Stueve
Don Sturek
Mark Sturza
Bo Sun
David Tepen
Mark-Rene Uchida
James Van De Ligt
John Vergis
Billy Verso
David Wallace
Xiaohui Wang
Stephen Webb
Karl Weber
Scott Willy
Chun Yu Charles Wong
Yu Yuan
Oren Yuen

When the IEEE SA Standards Board approved this standard on 9 May 2021, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Edward A. Addy
Doug Edwards
Ramy Ahmed Fathy
J. Travis Griffith
Thomas Koshy
Joseph L. Koepfinger*
David J. Law
Howard Li
Daozhuang Lin
Kevin Lu
Daleep C. Mohla
Chenhui Niu
Damir Novosel
Annette Reilly
Dorothy Stanley
Mehmet Ulema
Lei Wang
F. Keith Waters
Karl Weber
Sha Wei
Howard Wolfman
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.15.4y-2021, IEEE Standard for Low-Rate Wireless Networks—Amendment 3: Advanced Encryption Standard (AES)-256 Encryption and Security Extensions.

This amendment defines security extensions to IEEE Std 802.15.4 to add at a minimum AES-256-CCM as well as define possible methods of adding future encryption modes and key lengths (algorithm agility) as part of this amendment. The current IEEE 802.15.4 standard supports either AES-128-CCM or no security.

This amendment does not have any bits on the air changes to the current standard IEEE Std 802.15.4-2020 (i.e., all old implementations of the standard will see frames just like any frames where they do not have an appropriate security key). All tools that monitor, record, or replay IEEE 802.15.4 traffic will work with this amendment without any changes.

Contents

IEEE Standard for Low-Rate Wireless Networks

Amendment 3: Advanced Encryption Standard (AES)-256 Encryption and Security Extensions

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. 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.

3. Definitions, acronyms, and abbreviations

3.2 Acronyms and abbreviations

Insert the following acronym in alphabetical order:

IANA	Internet Assigned Numbers Authority

8. MAC services

8.2 MAC management service

8.2.2 Common requirements for MLME primitives

Insert the following new generic security errors alphabetically in the list that follows paragraph three:

— KEY_LENGTH_MISMATCH: Returned when the *secKey* within the *secKeyDescriptor* has a length that is inconsistent with the *secAeadAlgorithm.*