IEEE STANDARDS ASSOCIATION

# IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices

IEEE Computer Society

Sponsored by the
Cybersecurity and Privacy Standards Committee

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

**IEEE Std 1619.1™-2018**
(Revision of
IEEE Std 1619.1-2007)

**IEEE Std 1619.1™-2018**
(Revision of
IEEE Std 1619.1-2007)

# IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices

Sponsor

**Cybersecurity and Privacy Standards Committee**

**IEEE Computer Society**

Approved 23 October 2018

**IEEE-SA Standards Board**

**Abstract:** Cryptographic and data authentication procedures for storage devices that support length expansion, such as tape drives, are specified. Such procedures include the following cryptographic modes of operation for the AES block cipher: CCM, GCM, CBC-HMAC, and XTS-HMAC.

**Keywords:** authentication, CBC, CCM, cryptography, data storage, encryption, GCM, HMAC, IEEE 1619.1™, security, tape drive, variable-length block, XTS

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



PDF: ISBN 978-1-5044-5454-4 STD23493
Print: ISBN 978-1-5044-5455-1 STDPD23493

## 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 Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/ipr/disclaimers.html.

## 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. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups 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 Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. 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.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

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

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

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

## Translations

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

## Official statements

A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

## Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

## Laws and regulations

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

## Copyrights

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

## Photocopies

Subject to payment of 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. A current 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 IEEE Xplore at http://ieeexplore.ieee.org/ 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.

## Participants

At the time this IEEE standard was completed, the Security in Storage Working Group had the following membership:

**Walt Hubis,** *Chair*
**Eric Hibbard,** *Vice Chair*

| | | |
|---|---|---|
| Mohsin Awan | James Hatfield | Thomas Rivera |
| Tim Chevalier | Glen Jaquette | Robert Strong |

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

| | | |
|---|---|---|
| Johann Amsenga | Werner Hoelzl | Venkatesha Prasad |
| Demetrio Bucaneg Jr. | Noriyuki Ikeuchi | Thomas Starai |
| John Geldman | Quist-Aphetsi Kester | Walter Struppler |
| Randall Groves | Kenneth Lang | Oren Yuen |

When the IEEE-SA Standards Board approved this standard on 23 October 2018, it had the following membership:

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

| | | |
|---|---|---|
| Ted Burse | Xiaohui Liu | Robby Robson |
| Guido R. Hiertz | Kevin Lu | Dorothy Stanley |
| Christel Hunter | Daleep Mohla | Mehmet Ulema |
| Joseph L. Koepfinger* | Andrew Myles | Phil Wennblom |
| Thomas Koshy | Paul Nikolich | Philip Winston |
| Hung Ling | Ronald C. Petersen | Howard Wolfman |
| Dong Liu | Annette D. Reilly | Jingyi Zhou |

*Member Emeritus

## Introduction

This introduction is not part of IEEE Std 1619.1-2018, IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices.

The problem of data storage protection has become increasingly important due to legislation that requires the protection of sensitive information. To address this issue, the Security in Storage Working Group (SISWG) is developing standards for the protection of information on storage media. This standard provides strong data protection by specifying encryption with authentication and length expansion.

This standard provides methods suitable for ensuring the privacy and integrity of stored data within applications requiring a high level of assurance. To this end, this standard specifies the Advanced Encryption Standard (AES) cipher as used in authenticated-encryption modes.

There are many modes of non-cryptographic attacks that are outside the scope of this standard. See B.1 for a discussion.

## Contents

# IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices

## 1. Overview

### 1.1 Scope

This standard specifies requirements for cryptographic units that provide encryption and authentication for data contained within storage media. Full interchange requires additional format specifications (such as compression algorithms and physical data format) that are beyond the scope of this standard.

### 1.2 Purpose

This standard is suitable for encryption of data stored on tape because tape easily accommodates length-expanding ciphertext. In addition, this standard applies to other storage devices if these support storing extra metadata with each encrypted record. The algorithms of this standard are designed to help ensure the confidentiality and integrity of stored data within systems requiring a high level of assurance.

### 1.3 Description of clauses and annexes

— Clause 1 provides an overview of this standard, including scope and purpose.

— Clause 2 lists the normative references that are essential for implementing this standard.

— Clause 3 gives definitions, acronyms, and abbreviations used in this standard.

— Clause 4 provides a description of the components that play roles in this standard.

— Clause 5 describes the cryptographic modes used by the cryptographic unit.

— Clause 6 describes cryptographic key management and initialization vector requirements.

— Annex A (informative) lists bibliographic references that are useful when implementing this standard.

— Annex B (informative) discusses several security issues that an implementer and user should understand.

— Annex C (informative) provides a summary of documentation requirements.

— Annex D (informative) provides several test vectors useful in verifying a cryptographic unit.