



IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices

IEEE Computer Society

Sponsored by the
Storage Systems Standards Committee
and
Information Assurance Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA
16 May 2008

IEEE Std 1619.1™-2007

IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices

Sponsor
Information Assurance Standards Committee
and
Storage Systems Standards Committee
of the
IEEE Computer Society

Approved 15 April 2008
American National Standards Institute

Approved 5 December 2007
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, security, tape drive, variable-length block, XTS

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

Copyright © 2008 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 16 May 2008. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent and Trademark Office, owned by the Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-5360-5 STD95753
Print: ISBN 978-0-7381-5361-2 STDPD95753

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 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. When a document is more than five years old and has not been reaffirmed, 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. 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. Comments 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 1619.1-2007, 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.

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/reading/ieee/updates/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/reading/ieee/interp/index.html>.

Patents

Attention is called to the possibility that implementation of this guide may require use of subject matter covered by patent rights. By publication of this guide, 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 guide 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

When work on this standard began, the Security in Storage Working Group had the following officers:

James P. Hughes, *Chair*

Serge Plotkin, *Vice-chair*

Fabio Maino, *Secretary*

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Security in Storage Working Group operated under the following sponsorship:

John L. Cole, *Sponsor*

Curtis Anderson, *Co-Sponsor*

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Security in Storage Working Group had the following officers:

Matthew V. Ball, *Chair*

Eric A. Hibbard, *Vice-chair*

Fabio Maino, *Secretary*

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the P1619.1 Task Group had the following membership:

Matthew V. Ball, *Chair, Technical Editor*

Gideon Avida
 Matthew V. Ball
 Mark Benedikt
 Jon Buckingham
 William G. Colvin
 Russel S. Dietz
 Robert Drennan
 Hal Finney
 John Geldman
 Robert W. Griffin
 Shai Halevi (*past technical editor*)
 Laszlo Hars

Eric A. Hibbard
 Larry D. Hofer
 Jon Holdman
 Walter A. Hubis
 James P. Hughes (*past technical editor*)
 Glen Jaquette (*past technical editor*)
 Curt Kolovson
 Robert A. Lockhart
 Fabio R. Maino
 Charlie Martin
 Dalit Naor

Landon Curt Noll
 Jim Norton
 Scott Painter
 David Peterson
 Serge Plotkin
 David B. Sheehy
 Robert N. Snively
 Alexander (Sandy) Stewart
 Greg Unruh
 Douglas L. Whiting
 Christopher L. Williams
 Mike Witkowski

Special thanks to Brian Gladman, David McGrew, Michael Torla, and Danh Tran

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

Danilo Antonelli
 Matthew V. Ball
 Rahul B. Bhushan
 Juan C. Carreon
 Lidong Chen
 Keith Chow
 Roger Cummings
 Geoffrey Darnton
 Russell S. Dietz
 Thomas J. Dineen
 Robert C. Elliott
 Michael D. Geipel
 John Geldman
 Brian Goodman

Robert W. Griffin
 Randall Groves
 Eric A. Hibbard
 Werner Hoelzl
 Larry D. Hofer
 Walter A. Hubis
 Raj Jain
 Robert A. Lockhart
 William Lumpkins
 Fabio R. Maino
 Edward McCall
 Michael Newman
 Landon Curt Noll
 Mark Overby

Serge Plotkin
 Ulrich Pohl
 Venkatesha Prasad
 Michael D. Rush
 David B. Sheehy
 Avraham Shimor
 Robert N. Snively
 Thomas Starai
 Walter Struppler
 Joseph Tardo
 Wen Tong
 Thomas Tullia
 Christopher L. Williams
 Oren Yuen

When the IEEE-SA Standards Board approved this standard on 5 December 2007, it had the following membership:

Steve M. Mills, *Chair*
Robert M. Grow, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Richard DeBlasio
 Alex Gelman
 William R. Goldbach
 Arnold M. Greenspan
 Joanna N. Guenin
 Julian Forster*
 Kenneth S. Hanus
 William B. Hopf

Richard H. Hulet
 Hermann Koch
 Joseph L. Koepfinger*
 John Kulick
 David J. Law
 Glenn Parsons
 Ronald C. Petersen
 Tom A. Prevost

Narayanan Ramachandran
 Greg Ratta
 Robby Robson
 Anne-Marie Sahazizian
 Virginia C. Sulzberger
 Malcolm V. Thaden
 Richard L. Townsend
 Howard L. Wolfman

*Member Emeritus

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

Satish K. Aggarwal, *NRC Representative*
 Alan H. Cookson, *NIST Representative*

Lorraine Patsco
IEEE Standards Program Manager, Document Development

Michael Kipness
IEEE Standards Program Manager, Technical Program Development

CONTENTS

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
1.3 Description of clauses and annexes	1
2. Normative references.....	2
3. Keywords, definitions, acronyms, and abbreviations	2
3.1 Keywords.....	2
3.2 Definitions	3
3.3 Acronyms and abbreviations	6
3.4 Mathematical conventions	6
4. General concepts	6
4.1 Introduction	6
4.2 Components	8
4.3 Plaintext record formatter	10
4.4 Plaintext record de-formatter	10
4.5 Encryption routine	11
4.6 Decryption routine	11
4.7 Cryptographic parameters.....	13
5. Cryptographic modes.....	13
5.1 Overview	13
5.2 Counter with cipher block chaining-message authentication code (CCM).....	14
5.3 Galois/Counter Mode (GCM).....	15
5.4 Cipher block chaining with keyed-hash message authentication code (CBC-HMAC)	15
5.5 Xor-encrypt-xor with tweakable block-cipher with keyed-hash message authentication code (XTS-HMAC).....	17
6. Cryptographic key management and initialization vector requirements.....	19
6.1 Random bit generator	19
6.2 Cryptographic key entry and export	20
6.3 Handling the cipher key.....	20
6.4 Cryptographic key wrapping on the storage medium	20
6.5 Initialization vector (IV) requirements	21
6.6 Creating unique IVs within a self-contained group	22
Annex A (informative) Bibliography	24
Annex B (informative) Security concerns	26
B.1 Threat model	26
B.2 Maintaining cryptographic key security.....	26
B.3 Replay attacks	27

B.4 Passing plaintext to the host before checking the MAC	27
B.5 Checking for integrity of a cryptographic key	28
B.6 Avoiding collisions of initialization vectors	28
B.7 Examples of IV collision avoidance strategies	28
B.8 How many records to encrypt with one key?	30
Annex C (informative) Documentation summary	32
Annex D (informative) Test vectors	33
D.1 General.....	33
D.2 CCM-128-AES-256 test vectors.....	34
D.3 GCM-128-AES-256 test vectors.....	35
D.4 CBC-AES-256-HMAC-SHA test vectors (including HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512)	38
D.5 XTS-AES-256-HMAC-SHA-512 test vectors.....	41

IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices

IMPORTANT NOTICE: This standard is not intended to assure safety, security, health, or environmental protection in all circumstances. 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>.

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 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.

2. Normative references

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 1619TM, IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices.^{1, 2}

McGrew, David and John Viega, The Galois/Counter Mode of Operation (GCM), May 31, 2005.³

NIST FIPS 180-2, Federal Information Processing Standard (FIPS) 180-2 (August 1, 2002), Announcing the Secure Hash Standard (SHA).⁴

NIST FIPS 197, Federal Information Processing Standard (FIPS) 197 (November 26, 2001), Announcing the Advanced Encryption Standard (AES).

NIST FIPS 198, Federal Information Processing Standard (FIPS) 198 (March 2002 updated April 8, 2002), The Keyed-Hash Message Authentication Code (HMAC).

NIST Special Publication 800-38A (NIST SP 800-38A), Recommendation for Block Cipher Modes of Operation—Methods and Techniques.

NIST Special Publication 800-38C (NIST SP 800-38C), Recommendation for Block Cipher Modes of Operation: The CCM mode for authentication and confidentiality.

3. Keywords, definitions, acronyms, and abbreviations

3.1 Keywords

For the purposes of this standard, the following terms are keywords.

can: A keyword indicating a capability (*can* equals *is able to*).

required: *See shall.*

may: A keyword indicating a course of action permissible within the limits of this standard (*may* equals *is permitted to*).

¹ IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (<http://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 Available from the World Wide Web site <http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf> or http://siswg.org/docs/gcm_spec.pdf

⁴ Available from the NIST World Wide Web site <http://csrc.nist.gov/>

must: A keyword used only to describe an unavoidable situation that does not constitute a requirement for compliance to this standard.

shall: A keyword indicating a mandatory requirement strictly to be followed in order to conform to this standard and from which no deviation is permitted. (*shall equals is required to*).

shall not: A phrase indicating an absolute prohibition of this standard.

should: A keyword indicating that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is deprecated but not prohibited (*should equals is recommended to*).

3.2 Definitions

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards, Seventh Edition*, [B6]⁵ should be referenced for terms not defined in this clause.

3.2.1 additional authenticated data (AAD): Information passed into an authenticated encryption routine that is authenticated but not encrypted.

3.2.2 advanced encryption standard (AES): The block cipher defined by NIST FIPS 197. *See also:* **block cipher**.

3.2.3 block cipher: A cryptographic primitive that uses a cipher key to create a pseudo-random permutation of a fixed-size bit string. *See also:* **cipher key; plaintext; ciphertext**.

3.2.4 cipher block chaining (CBC): A cryptographic mode of operation in which the ciphertext output from each cipher block feeds into the following cipher block (see NIST SP 800-38A).

3.2.5 cipher block chaining initialization vector (CBC-IV): The IV input for the CBC modes, according to NIST SP 800-38A. *See also:* **CBC-HMAC; initialization vector**.

NOTE—See 5.4.⁶

3.2.6 cipher block chaining with keyed-hash message authentication code (CBC-HMAC): A family of cryptographic modes that uses the cipher block chaining (CBC) mode (see NIST SP 800-38A) for confidentiality and a key-hash message authentication code (HMAC) for integrity (see NIST FIPS 198).

3.2.7 cipher block chaining with keyed-hash message authentication code using secure hash algorithm (CBC-HMAC-SHA): A family of cipher blocking chaining (CBC) modes (see NIST SP 800-38A) with a keyed-hash message authentication code (see NIST FIPS 198) from a member of the secure hash algorithm family (see NIST FIPS 180-2).

NOTE—See 5.4.

3.2.8 cipher key: A bit string that controls the pseudo-random permutation of a encryption or decryption routine. *See also:* **cryptographic key; block cipher**.

3.2.9 ciphertext record: The result of encrypting a same-length plaintext record using a cryptographic mode of operation. *See also:* **ciphertext; cryptographic mode of operation; plaintext record**.

⁵ The numbers in brackets correspond to those of the bibliography in Annex A.

⁶ Notes in text, tables, and figures are given for information only, and do not contain requirements needed to implement the standard.

3.2.10 collision: An event where two independent variables have the same value in a particular context. *See also:* **initialization vector; plaintext; ciphertext.**

3.2.11 counter mode (CTR): A cryptographic mode of operation defined by NIST SP 800-38A in which the ciphertext is the bitwise exclusive-OR of the plaintext with an encrypted counter.

3.2.12 counter with cipher block chaining message authentication code (CCM): A cryptographic mode of operation that provides confidentiality with counter mode and integrity with a message authentication code that uses cipher block chaining (see NIST SP 800-38C).

NOTE—See 5.2.

3.2.13 cryptographically-sound random-bit generator (RBG): A device or algorithm that outputs a sequence of binary bits that appears to be statistically independent and unbiased. In particular, a RBG generates numbers that are highly unpredictable, and knowledge of any particular output from a RBG does not reveal any information about other data generated by the RBG.

NOTE—See 6.1.

3.2.14 cryptographic hash function: A hash function that generates a hash value from an input and that has the following properties: 1) it is computationally difficult to compute the inverse (i.e., compute the input from the hash value); 2) it is computationally difficult to find two different inputs that have the same hash value; 3) it is computationally difficult to find an input whose hash value is a particular value.

3.2.15 cryptographic key: A bit string used as an input into cryptographic primitives. *See also:* **block cipher; cipher key.**

3.2.16 cryptographic mode: *See cryptographic mode of operation.*

3.2.17 cryptographic mode of operation: An algorithm that includes a block cipher used in a particular configuration and uses a cipher key to convert plaintext into ciphertext and vice versa. *See also:* **block cipher; cipher key; plaintext; ciphertext.**

3.2.18 cryptographic unit: Any set of software, firmware, or hardware that can perform a cryptographic operation.

3.2.19 decryption: The act of producing plaintext from ciphertext. *Contrast:* **encryption.** *See also:* **plaintext; ciphertext; cryptographic key; cryptographic mode of operation.**

3.2.20 decryption routine: An instantiation of a cryptographic mode of operation that converts ciphertext into plaintext.

3.2.21 encrypted record: A collection of fields that includes the output of an encryption operation or authentication operation (e.g., ciphertext, message authentication code), and optionally contains other information needed for a subsequent decryption operation (e.g., additional authenticated data, initialization vector). *See also:* **ciphertext; initialization vector; message authentication code; additional authenticated data.**

3.2.22 encryption: The act of producing ciphertext from plaintext. *Contrast:* **decryption.** *See also:* **plaintext; ciphertext; cryptographic key; cryptographic mode of operation.**

3.2.23 encryption routine: An instantiation of a cryptographic mode of operation that converts plaintext into ciphertext.

3.2.24 encryption session: An interval in which a cryptographic unit generates encrypted records using a set of self-consistent variables, such as unique initialization vectors. *See also:* **encryption; initialization vector; cryptographic unit.**

NOTE—See 6.5.3.

3.2.25 Galois/Counter Mode (GCM): A cryptographic mode of operation that provides confidentiality through counter mode encryption and integrity through a message authentication code that uses Galois field arithmetic. (See McGrew and Viega, The Galois/Counter Mode of Operation.)

NOTE—See 5.3.

3.2.26 host record: A string of plaintext passed to the cryptographic unit from the host. *See also:* **plaintext record; cryptographic unit; host.**

3.2.27 initialization vector (IV): An input into an encryption or decryption algorithm that needs not be secret, but has a high probability of being unique when used with a particular cipher key. *See also:* **encryption; decryption; encryption session; cipher key.**

NOTE—See 6.5.

3.2.28 key encrypting key (KEK): A cryptographic key used only for encrypting or decrypting other cryptographic keys. *See also:* **cryptographic key; encryption.**

3.2.29 keyed-hash message authentication code (HMAC): A message authentication code defined by NIST FIPS 198 that includes a secret hash key.

3.2.30 key manager: Any device or person that controls the creation, archiving, and destruction of cryptographic keys. *See also:* **cryptographic key.**

NOTE—See 4.2.3.

3.2.31 message authentication code (MAC): A cryptographic checksum that is used to detect intentional modifications and errors in an encrypted record, and cannot be efficiently forged without knowledge of the cryptographic key used in the MAC algorithm. *See also:* **encrypted record.**

3.2.32 nonce: A bit string that has a low probability of matching any other nonce in a particular context. *See also:* **initialization vector.**

3.2.33 plaintext: Information that has not been obscured through a cryptographic transformation. *Contrast:* **ciphertext.**

3.2.34 plaintext record: A string of plaintext passed to an encryption routine to produce a same-length ciphertext record. *See also:* **plaintext; cryptographic unit; encryption; encrypted record; host record.**

3.2.35 policies: In cryptography, a set of rules that defines aspects of the management of a cryptographic system (e.g., encryption, decryption, or bypass rules).

3.2.36 random bit generator (RBG): *See* **cryptographically-sound random-bit generator.**

3.2.37 random nonce: A nonce that completely consists of the output from a random bit generator. *See also:* **nonce; cryptographically-sound random-bit generator.**

3.2.38 Secure Hash Algorithm (SHA): A family of cryptographic hash functions defined by NIST FIPS 180-2. *See also* **cryptographic hash function.**

3.2.39 self-contained group: A set of cryptographic units that generate and use IVs in a consistent manner.

3.2.40 Xor-encrypt-xor with tweak and ciphertext stealing (XTS): The cryptographic mode of operation described in IEEE Std 1619.

NOTE—See 6.6.

3.3 Acronyms and abbreviations

AAD	additional authenticated data
AES	advanced encryption standard
CBC	cipher block chaining
CCM	counter with cipher block chaining message authentication code
CTR	counter mode
FIPS	Federal Information Processing Standards
GCM	Galois/Counter Mode
HMAC	keyed-hash message authentication code
IEEE	Institute of Electrical and Electronics Engineers
IV	initialization vector
KEK	key encrypting key
MAC	message authentication code
NIST	National Institute of Standards and Technology
RBG	(cryptographically-sound) random-bit generator
SHA	Secure Hash Algorithm
SP	(NIST) special publication
XOR	exclusive OR
XTS	xor-encrypt-xor with tweak and ciphertext stealing

3.4 Mathematical conventions

This standard uses decimal, binary, and hexadecimal numbers. For clarity, decimal numbers generally represent counts, and binary or hexadecimal numbers describe bit patterns or raw binary data.

Binary numbers are represented by a string of one or more binary digits, followed by the subscript 2. For example, the decimal number 26 is represented as 00011010₂ in binary.

4. General concepts

4.1 Introduction

This standard describes elements of an architecture that is suitable for the cryptographic confidentiality and integrity of stored data. This architecture includes a model of several components within a typical system that securely stores and retrieves information. These components are as follows:

- A *controller* that controls the overall operation of the cryptographic unit and receives status from the cryptographic unit (see 4.2.1)
- A *host* that provides plaintext data, in the form of host records, to the cryptographic unit and receives plaintext data from the cryptographic unit (see 4.2.2)
- A *key manager* that may provide or negotiate *cipher keys* and/or *key encrypting keys* (KEK) to the cryptographic unit, and that should securely maintain the lifecycle of these cryptographic keys (see 4.2.3)
- A *cryptographic unit* that performs data formatting, encryption, and decryption, and that may perform cryptographic key management (see 4.2.4)
- A *storage medium* that provides non-volatile storage of encrypted records and metadata produced by the cryptographic unit (see 4.2.5)