IEEE Standard for
Local and metropolitan area networks—

Part 21: Media Independent Services Framework—Corrigendum 1: Clarification of Parameter Definition in Group Session Key Derivation

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.21™-2017/Cor 1-2017
(Corrigendum to
IEEE Std 802.21-2017)

IEEE Standard for
Local and metropolitan area networks—

Part 21: Media Independent Services Framework—Corrigendum 1: Clarification of Parameter Definition in Group Session Key Derivation

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 6 December 2017

IEEE-SA Standards Board

Abstract: This corrigendum provides technical and editorial corrections to IEEE Std 802.21-2017.

Keywords: group, group session key, IEEE 802.21™, master group key, media independent session key

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

PDF: ISBN 978-1-5044-4624-2 STD22959

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. 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/ 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 corrigendum was submitted to the IEEE-SA Standards Board for approval, the IEEE P802.21 Working Group had the following membership:

Subir Das, *Chair*
Hyeong Ho Lee, *Vice Chair*
Yoshikazu Hanatani, *Technical Editor*

Clint Chaplin
Lidong Chen
Sangkwon Peter Jeong
Farrokh Khatibi
Heeseob Lee
Changhwa Lyou
Karen Randall
Yusuke Shimizu
Dong II Seo
Tomoki Takazoe

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

Iwan Adhicandra
Thomas Alexander
Butch Anton
Harry Bims
Demetrio Bucaneg Jr.
William Byrd
Juan Carreon
Lidong Chen
Charles Cook
Daniel Corujo
Subir Das
Sourav Dutta
Avraham Freedman
Eric W. Gray
Randall Groves
Yoshikazu Hanatani
Robert Heile
Werner Hoelzl
Noriyuki Ikeuchi
Atsushi Ito
Raj Jain
SangKwon Jeong
Piotr Karocki
Stuart Kerry
Yongbum Kim
Yasushi Kudoh
Hyeong Ho Lee
Stephen McCann
Nick S.A Nikjoo
Arumugam Paventhan
Venkatesha Prasad
Karen Randall
Maximilian Riegel
Robert Robinson
Thomas Starai
Michael Stelts
Walter Struppler
Tomoki Takazoe
Mark-Rene Uchida
Oren Yuen

When the IEEE-SA Standards Board approved this corrigendum on 6 December 2017, it had the following membership:

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

Chuck Adams
Masayuki Ariyoshi
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Michael Janezic
Thomas Koshy
Joseph L. Koepfinger*
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 802.21-2017/Cor 1-2017, IEEE Standard for Local and metropolitan area networks—Part 21: Media Independent Services Framework—Corrigendum 1: Clarification of Parameter Definition in Group Session Key Derivation.

This corrigendum provides technical clarifications and editorial corrections to the parameter definition in group session key derivation published in IEEE Std 802.21-2017.

Contents

IEEE Standard for
Local and metropolitan area networks—

Part 21: Media Independent Services Framework—Corrigendum 1: Clarification of Parameter Definition in Group Session Key Derivation

NOTE—The editing instructions contained in this corrigendum 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.

9. MIS protocol protection

9.6 Group addressed message protection

Change 9.6.1 as follows:

9.6.1 Group session key derivation

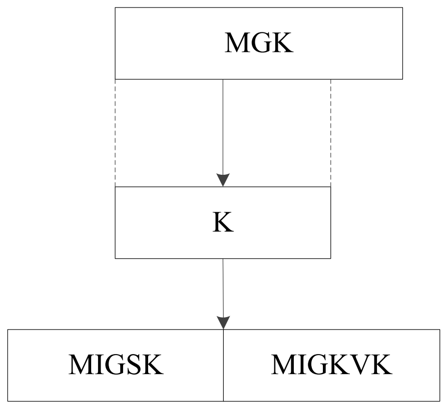

Figure 73—Key derivation example

When a recipient of a GKB successfully decrypts an MGK from the GKB, a media independent group session key (MIGSK) is derived from the MGK to protect group manipulation commands and group addressed commands:

For the key derivation, the following notations and parameters are used:

— *K*: key derivation key. It is truncated from a master group key (MGK). The length of *K* is determined by the pseudorandom function (PRF) used for key derivation. If HMAC-SHA-1 or HMAC-SHA-256 is used as a PRF, then the full MGK is used as key derivation key, *K*. If CMAC-AES is used as a PRF, then the first 128 bits of MGK are used as derivation key, *K*.

— *L*: The binary length of derived keying material MIGSK and MIGKVK. $L = L1 + L2$; where $L1$ is determined by selected group ciphersuite (described in 9.6.5) and $L2$ is determined by group key distribution ciphersuites (described in 9.6.6).

— *h*: The output binary length of PRF used in the key derivation. That is, *h* is the length of the block of the keying material derived by one PRF execution. Specifically, for HMAC-SHA-1, h = 160 bits; for HMAC-SHA-256, h = 256 bits; for CMAC-AES, h = 128 bits.

— *n*: The number of iterations of PRF in order to generate *L*-bits keying material.

— *c*: The group ciphersuite code is a one octet string specified for each ciphersuite. The code is defined in 9.6.5.

— *v*: The length of the binary representation of the counter and the length of keying material *L*. The default value for *v* is 32.

— “MIGSK”: 0x4D4947534B, ASCII code in hex for string “MIGSK.”

— $[a]_2$: Binary representation of integer *a* with a given length.

For given PRF, the key derivation for MIGSK and MIGKVK can be described in the following procedures:

Fixed input values: *h* and *v*.

Input: *K*, *L*, and group ciphersuite code.

Process:

a) $n := \lceil L/h \rceil$

b) If $n > 2^v - 1$, then indicate an error and stop.

c) Result(0) := empty string.

d) For i = 1 to *n*, do

  1) K(i) := PRF(K, “MIGSK” || $[\mathrm{i}]_2$ || c || $[L]_2$).

  2) Result(i) = Result(i − 1) || K(i).

e) Return Result(*n*). ~~and~~ MIGSK is the leftmost ~~*L*~~ bits of Result(*n*) and its length is represented as *L*1. MIGKVK is the remaining leftmost bits of Result(*n*) and its length is represented as *L*2. If *L*2 is ‘0’, MIGKVK is not included.

Output: MIGSK || MIGKVK.

With the above procedure, a key hierarchy is derived as shown in Figure 73.

This mechanism conforms with NIST SP800-108 (KDF in Counter Mode).

9.6.5 Group ciphersuites

Change* Table 27 *as follows:

Table 27—Group ciphersuites

Code	Encryption algorithm	Digital signature algorithm	*L1*
10000100	NULL	ECDSA-256	0
10010001	AES_CCM-128	NULL	128
10010101	AES_CCM-128	ECDSA-256	128

9.6.6 Group key distribution ciphersuites

Change* Table 28 *as follows:

Table 28—Group key distribution ciphersuites

Code	Wrapping algorithm	MAC algorithm for VerifyGroupCode	*L2*
11010100	AES_Key_Wrapping-128	NULL	0
11000100	AES_ECB-128	NULL	0
11000101	AES_ECB-128	AES-CMAC-128	128
11000000	No group key distribution	NULL	0

Consensus

WE BUILD IT.

Connect with us on:

Facebook: https://www.facebook.com/ieeesa

Twitter: @ieeesa

LinkedIn: http://www.linkedin.com/groups/IEEESA-Official-IEEE-Standards-Association-1791118

IEEE-SA Standards Insight blog: http://standardsinsight.com

YouTube: IEEE-SA Channel

IEEE
standards.ieee.org
Phone: +1 732 981 0060 Fax: +1 732 562 1571