P802.1AEbt/D0.3

DRAFT Amendment to IEEE Std 802.1AE–2006

Draft Standard for

Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 2: Extended Packet Numbering

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

DRAFT FOR DISCUSSION OF PROPOSED PAR

~~**Prepared by the Security Task Group of IEEE 802.1**~~

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

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.

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
P.O. Box 13 31
Piscataway, NJ 08855-1331
USA

Note: 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 with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Editors' Foreword

<<Notes>>

<<Throughout this document, all notes such as this one, presented between angle braces, are temporary notes inserted by the Editors for a variety of purposes; these notes and the Editors' Foreword will all be removed prior to publication and are not part of the normative text.>>

<<Comments and participation in 802.1 standards development

Comments on this draft are encouraged. **PLEASE NOTE: All issues related to IEEE standards presentation style, formatting, spelling, etc. are routinely handled between the 802.1 Editor and the IEEE Staff Editors prior to publication, after balloting and the process of achieving agreement on the technical content of the standard is complete.** Readers are urged to devote their valuable time and energy only to comments that materially affect either the technical content of the document or the clarity of that technical content. Comments should not simply state what is wrong, but also what might be done to fix the problem.>>

Full participation in the development of this draft requires individual attendance at IEEE 802 meetings. Information on 802.1 activities, working papers, and email distribution lists etc. can be found on the 802.1 Website:

http://ieee802.org/1/

Use of the email distribution list is not presently restricted to 802.1 members, and the working group has had a policy of considering ballot comments from all who are interested and willing to contribute to the development of the draft. Individuals not attending meetings have helped to identify sources of misunderstanding and ambiguity in past projects. Non-members are advised that the email lists exist primarily to allow the members of the working group to develop standards, and are not a general forum. All contributors to the work of 802.1 should familiarize themselves with the IEEE patent policy and anyone using the mail distribution will be assumed to have done so. Information can be found at http://standards.ieee.org/db/patents/

Comments on this document may be sent to the 802.1 email exploder, to the Editor, or to the Chairs of the 802.1 Working Group and Security Task Group.

Email:

Mick Seaman
Editor, P802.1AE
Chair, 802.1 Security Task Group
Email:mick_seaman@sbcglobal.net

Tony Jeffree
Chair, 802.1 Working Group
11A Poplar Grove
Sale, Cheshire, M33 3AX, UK
+44 161 973 4278 (Tel)
+44 161 973 6534 (Fax)
Email: tony@jeffree.co.uk

PLEASE NOTE: Comments whose distribution is restricted in any way cannot be considered, and may not be acknowledged.>>

<<Overview: Draft text and accompanying information

This document currently comprises:

A cover page, identical to the title page.
The editors' introductory notes to each draft, briefly summarizing the progress and focus of each successive draft.
The title page for this amendment including an Abstract and Keywords. This title page will be retained for the period that the amendment is published as a separate document.
The amendment proper, documented in the usual form for amendments to 802 standards; i.e., as an explicit set of editing instructions that, if correctly applied to the text of 802.1Q, will create a corrected document.
An Annex Z comprising the editors' discussion of issues. This annex will be deleted from the document prior to sponsor ballot.
Editors' notes throughout the document, including requests for comment on specific issues and pointing deficiencies in the current draft.
IEEE boilerplate text.

The records of participants in the development of the standard, the introduction to 802 standards, and the introduction to this revision of the standard are not included, and will be added at an appropriate time.

During the early stages of draft development, 802.1 editors have a responsibility to attempt to craft technically coherent drafts from the resolutions of ballot comments and the other discussions that take place in the working group meetings. Preparation of drafts often exposes inconsistencies in editor's instructions or exposes the need to make choices between approaches that were not fully apparent in the meeting. Choices and requests by the editors' for contributions on specific issues will be found in the editors' introductory notes to the current draft, at appropriate points in the draft, and in Annex Z. Significant discussion of more difficult topics will be found in the last of these.

The ballot comments received on each draft, and the editors' proposed and final disposition of comments on working group drafts, are part of the audit trail of the development of the standard and are available, along with all the revisions of the draft on the 802.1 website (for address see above).

During the early stages of draft development the proposed text can be moved around a great deal, and even minor rearrangement can lead to a lot of 'change', not all of which is noteworthy from the point of the reviewer, so the use of automatic change bars is not very effective. In this draft change bars have been manually applied, with a view to drawing the readers attention to the most significant areas of change. Readers interested in viewing every change are encouraged to used Adobe Acrobat to compare the document with their selected prior draft.
>>

<<Editor's Introduction to the current draft.

This document has no official standing, it has been prepared to facilitate discussion of a proposed PAR to amend 802.1AE to include extended packet numbering. It shows the nature and extent of changes that might result from an ensuing project.

With this amendment the PN can be either 32-bit or 64-bit (varying by Cipher Suite). Descriptions of the frame format explain that only the low-order 32 bits of the PN are carried in the MACsec frame.

Some key points:

— No frame format changes
— No MIB changes
— No conformance clause changes (yet, anyway) as the inclusion of additional Cipher Suites is already provided for in the existing MIB
— "Standalone" i.e. can be run as a project and yield a benefit without 802.1X amendment, though the latter is necessary to get in-service software upgrades

>>

<<Editor's Introduction to prior drafts (excerpts of continuing relevance).

>>

<<Project Authorization Request, Scope, Purpose, and Five Criteria

A suggestion for a proposed PAR (Project Authorization Request) for this project follows.

Scope of Proposed Project:

This standard specifies the optional use of AES-128 and AES-256 GCM (Galois Counter Mode) Cipher Suites that make use of a 64-bit PN (packet number) as part of their IV (Initial Value) parameter while retaining the existing MACsec frame format by communicating only the least significant 32 bits in the SecTAG.

Purpose of Proposed Project:

This standard specifies the optional use of Cipher Suites that make use of a 64-bit PN to allow more than 2^{32} packets to be sent with a single Secure Association Key.

Need for the Project:

At very high speeds (100 Gb/s and above) the existing MACsec Cipher Suites can exhaust an SAK, thus demanding rekeying, at a rate (~9 seconds for full utilization with minimum Ethernet frame sizes at 400 Gb/s) that may conflict with some organizations' security policies and allowing inadequate time for in-service software upgrades that temporarily suspend key agreement protocol operation. There is significant broad interest in the use of MACsec at these speeds and a desire to address these issues while retaining a high degree of compatibility with existing implementations and deployment.

1. Broad Market Potential

A standards project authorized by IEEE 802 shall have a broad market potential. Specifically, it shall have the potential for:

a) *Broad sets of applicability.*
This amendment is applicable to all networks that are currently using or planning to use MACsec. The addition of this cipher suite will continue the appeal and applicability of IEEE 802.1AE for customers deploying or planning use of the fastest LAN technologies.
b) *Multiple vendors and numerous users*
A number of major equipment providers have indicated support for this amendment.
c) *Balanced costs (LAN versus attached stations)*
There is no imbalance of cost created by this amendment

2. Compatibility

IEEE 802 defines a family of standards. All standards shall be in conformance with the IEEE 802.1 Architecture, Management and Interworking documents as follows: 802 Overview and Architecture, 802.1D, 802.1Q and parts of 802.1f. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with 802.

Each standard in the IEEE 802 family of standards shall include a definition of managed objects which are compatible with systems management standards.

This amendment fits within the framework of IEEE 802.1AE-2006 without changes to the frame formats. Implementations that conform to the existing standard will remain conformant. A definition of managed objects is already included in the base standard and will be retained with little (if any) extension, as it already provides for the addition of new Cipher Suites without changes to the MIB.

3. Distinct Identity

Each IEEE 802 standard shall have a distinct identity. To achieve this, each authorized project shall be:

a) *Substantially different from other IEEE 802 standards.*

   IEEE 802.1AE is already a recognized and established standard.

b) *One unique solution per problem (not two solutions to a problem).*

   This project enhances IEEE 802.1AE to meet emerging and additional needs, it does not duplicate existing capabilities.

c) *Easy for the document reader to select the relevant specification.*

   IEEE Std 802.1AE is already an established reference for MAC Security.

For a project to be authorized, it shall be able to show its technical feasibility. At a minimum, the proposed project shall show:

a) *Demonstrated system feasibility.*

   The characteristics of the GCM-AES family of cipher suites is already well known. IEEE 802.1AE was one of the first vehicles for this technology. Extended packet numbering techniques similar to that proposed for this amendment have already been deployed for IP security.

b) *Proven technology, reasonable testing.*

   Technology for testing cryptographic modes of operations is well advanced.

c) *Confidence in reliability.*

   GCM-AES has been adopted by NIST. Extended packet numbering techniques have been used for other purposes. This project is expected to pose no new reliability challenges.

d) *Coexistence of 802 wireless standards specifying devices for unlicensed operation.*

   Not applicable.

5. Economic Feasibility

For a project to be authorized, it shall be able to show economic feasibility (so far as can reasonably be estimated), for its intended applications. At a minimum, the proposed project shall show:

a) *Known cost factors, reliable data.*

   The economic factors for adoption of this technology outweigh the estimated costs of implementing the solution.

b) *Reasonable cost for performance.*

   The economic factors for adoption of this technology outweigh the estimated costs of implementing the solution.

c) *Consideration of installation costs.*

   The economic factors for adoption of this technology outweigh the estimated costs of implementing the solution.

>>

<<Editors' final checklist (items noted in development, to be applied to final text.

P802.1AEbt/D0.3
DRAFT Amendment to IEEE Std 802.1AE–2006
November 1, 2011

Draft Standard for

Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 2: Extended Packet Numbering

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

DRAFT FOR DISCUSSION OF PROPOSED PAR

~~**Prepared by the Security Task Group of IEEE 802.1**~~

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: authorized port, confidentiality, data origin authenticity, integrity, 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

PDF: ISBN xxxx
Print: ISBN xxxx

Introduction

This introduction is not part of IEEE Std 802.1AExx-20xx, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security—Amendment 2: Extended Packet Numbering.

The first edition of IEEE Std 802.1AE was published in 2006. A first amendment, IEEE Std 802.1AEbn-2011, added the option of using the GCM-AES-256 Cipher Suite. This second amendment adds optional Cipher Suites, GCM-AES-XPN-128 and GCM-AES-XPN-256, that allow more than 2^{32} frames to be protected with a single Secure Association Key (SAK) and so ease the timeliness requirements on key agreement protocols for very high speed (100 Gb/s plus) operation.

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. Implementors 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 standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Contents

1.Overview 2

2.Normative references 3

3.Definitions 4

4.Abbreviations and acronyms 5

5.Conformance 6

5.1 Requirements terminology 6
5.2 Protocol Implementation Conformance Statement (PICS) 6
5.3 Required capabilities 6
5.4 Optional capabilities 7

6.Secure provision of the MAC Service 9

7.Principles of secure network operation 10

8.MAC Security Protocol (MACsec) 11

8.3 MACsec operation 11

9.Encoding of MACsec protocol data units 12

9.3 Security TAG 12
9.8 Packet Number (PN) 12
9.9 Secure Channel Identifier (SCI) 13

10.Principles of MAC Security Entity (SecY) operation 14

10.6 Secure frame verification 14
10.7 SecY management 15

11.MAC Security in Systems 18

12.MACsec and EPON 19

13.Management protocol 20

13.7 Use of the MIB with extended packet numbering 20

14.Cipher Suites 21

14.1 Cipher Suite use 21
14.4 Cipher Suite conformance 22
14.6 GCM–AES–256 23
14.7 GCM–AES–XPN-128 24
14.8 GCM–AES–XPN-256 25

Annex A (normative) PICS Proforma........ 27

Annex B (informative) Bibliography........ 28

Annex C (informative) MACsec Test Vectors........ 30

C.1 Integrity protection (54-octet frame)........ 31
C.2 Integrity protection (60-octet frame)........ 36
C.3 Integrity protection (65-octet frame)........ 39
C.4 Integrity protection (79-octet frame)........ 42
C.5 Confidentiality protection (54-octet frame)........ 45
C.6 Confidentiality protection (60-octet frame)........ 50
C.7 Confidentiality protection (61-octet frame)........ 53
C.8 Confidentiality protection (75-octet frame)........ 56

Figures

Figure 9-2 SecTAG format 12
Figure 14-1 Cipher Suite Protect and Validate operations 21

Tables

Table 14-1 MACsec Cipher Suites 22
Table C-1 Unprotected frame (example) 31
Table C-2 Integrity protected frame (example) 31
Table C-3 GCM-AES-128 Key and calculated ICV (example) 32
Table C-4 GCM-AES-256 Key and calculated ICV (example) 33
Table C-5 GCM-AES-XPN-128 Key and calculated ICV (example) 34
Table C-6 GCM-AES-XPN-256 Key and calculated ICV (example) 35
Table C-7 Unprotected frame (example) 36
Table C-8 Integrity protected frame (example) 36
Table C-11 GCM-AES-XPN-128 Key and calculated ICV (example) 37
Table C-12 GCM-AES-XPN-256 Key and calculated ICV (example) 38
Table C-13 Unprotected frame (example) 39
Table C-14 Integrity protected frame (example) 39
Table C-17 GCM-AES-XPN-128 Key and calculated ICV (example) 40
Table C-18 GCM-AES-XPN-256 Key and calculated ICV (example) 41
Table C-19 Unprotected frame (example) 42
Table C-20 Integrity protected frame (example) 42
Table C-23 GCM-AES-XPN-128 Key and calculated ICV (example) 43
Table C-24 GCM-AES-XPN-256 Key and calculated ICV (example) 44
Table C-25 Unprotected frame (example) 45
Table C-26 Confidentiality protected frame (example) 45
Table C-27 GCM-AES-128 Key, Secure Data, and ICV (example) 46
Table C-28 GCM-AES-256 Key, Secure Data, and ICV (example) 47
Table C-29 GCM-AES-XPN-128 Key, Secure Data, and ICV (example) 48
Table C-30 GCM-AES-XPN-256 Key, Secure Data, and ICV (example) 49
Table C-31 Unprotected frame (example) 50
Table C-32 Confidentiality protected frame (example) 50
Table C-35 GCM-AES-XPN-128 Key, Secure Data, and ICV (example) 51
Table C-36 GCM-AES-XPN-256 Key, Secure Data, and ICV (example) 52
Table C-37 Unprotected frame (example) 53
Table C-38 Confidentiality protected frame (example) 53
Table C-41 GCM-AES-XPN-128 Key, Secure Data, and ICV (example) 54
Table C-42 GCM-AES-XPN-256 Key, Secure Data, and ICV (example) 55
Table C-43 Unprotected frame (example) 56
Table C-44 Confidentiality protected frame (example) 56
Table C-47 GCM-AES-XPN-128 Key, Secure Data, and ICV (example) 57
Table C-48 GCM-AES-XPN-256 Key, Secure Data, and ICV (example) 58

Draft Standard for Local and Metropolitan Area Networks—

Media Access Control (MAC) Security

Amendment 2: Extended Packet Numbering

This amendment to IEEE Std 802.1AE-2006 allows more than 2^{32} MACsec protected frames to be sent using a single Secure Association Key (SAK) by enabling the use of a 64-bit Packet Number (PN) and specifying two Cipher Suites (GCM-AES-XPN-128 and GCM-AES-XPN-256) that use that extended packet numbering as part of their Initial Value (IV) construction. MACsec frame formats and principles of MAC Security Entity operation remain unchanged. Changes are applied to the base text of IEEE Std 802.1AE-2006 as amended by IEEE Std 802.1AEbn-2011.

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. 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

This amendment makes no changes to Clause 1 Overview.

2. Normative references

This amendment makes no changes to Clause 2 Normative References.

3. Definitions

Change the definition of packet number as follows:

3.27 packet number (PN): A monotonically increasing value ~~used to uniquely identify a MACsec frame in the sequence of frames transmitted using an SA~~ that is guaranteed unique for each MACsec frame transmitted using a given SAK.

Add the following definition(s), in the appropriate collating order:

3.28 Short Secure Channel Identifier (SSCI): A 32-bit identifier, distributed by key agreement protocol, that uniquely identifies an SCI within the context of all SecY's using a given SAK.

4. Abbreviations and acronyms

Add the following abbreviation(s), in the appropriate collating sequence.

SSCI Short SCI

5. Conformance

This amendment makes no changes to Clause 5 Conformance.

<<The full text of the existing clause is provided here for the time being to aid review.>>

A claim of conformance to this standard is a claim that the behavior of an implementation of a MAC Security Entity (SecY) meets the requirements of this standard as they apply to the operation of the MACsec protocol, management of its operation, and provision of service to the protocol clients of the SecY, as revealed through externally observable behavior of the system of which the SecY forms a part.

A claim of conformance may be a claim of full conformance, or a claim of conformance with Cipher Suite variance, as specified in 5.4.

Conformance to this standard does not ensure that the system of which the MAC Security implementation forms a part is secure, or that the operation of other protocols used to support MAC Security, such as key management and network management do not provide a way for an attacker to breach that security.

5.1 Requirements terminology

For consistency with existing IEEE and IEEE 802.1 standards, requirements placed upon conformant implementations of this standard are expressed using the following terminology:

a) ***shall*** is used for mandatory requirements;
b) ***may*** is used to describe implementation or administrative choices (may means is permitted to, and hence, may and may not mean precisely the same thing);
c) ***should*** is used for recommended choices (the behaviors described by should and should not are both permissible but not equally desirable choices).

The PICS proforma (see Annex A (normative)) reflects the occurrences of the words *shall*, *may*, and *should* within the standard.

The standard avoids needless repetition and apparent duplication of its formal requirements by using ***is***, ***is not***, ***are***, and ***are not*** for definitions and the logical consequences of conformant behavior. Behavior that is permitted but is neither always required nor directly controlled by an implementor or administrator, or whose conformance requirement is detailed elsewhere, is described by ***can***. Behavior that never occurs in a conformant implementation or system of conformant implementations is described by ***cannot***. The word ***allow*** is used as a replacement for the cliche Support the ability for, and the word ***capability*** means can be configured to.

5.2 Protocol Implementation Conformance Statement (PICS)

The supplier of an implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex A (normative) and shall provide the information necessary to identify both the supplier and the implementation.

5.3 Required capabilities

An implementation of a MAC Security Entity (SecY) for which conformance to this standard is claimed shall

a) Support the Controlled and Uncontrolled Ports, and use a Common Port as specified in Clause 10.

b) Support the MAC status and point-to-point parameters for the Controlled and Uncontrolled Ports as specified in 6.4, 6.5, and 10.7.

c) Process transmit requests from the Controlled Port as required by the specification of Secure Frame Generation (10.5).

d) Process receive indications from the Common Port as required by the specification of Secure Frame Verification (10.6), prior to causing receive indications at the Controlled Port.

e) Encode and decode MACsec PDUs as specified in Clause 9.

f) Use a globally unique 48-bit MAC Address and a 16-bit Port Identifier unique within the scope of that address assignment to identify the transmit SCI, as specified in 8.2.1.

g) Satisfy the performance requirements specified in Table 10-1 and 8.2.2.

h) Support the Layer Management Interface (LMI) operations required by the Key Agreement Entity as specified in Clause 10.

i) Provide the management functionality specified in 10.7.

j) Protect and validate MACsec PDUs by using Cipher Suites as specified in 14.1.

k) Support Integrity Protection using the Default Cipher Suite specified in Clause 14.

l) For each Cipher Suite implemented, support a minimum of

   1) One receive SC

   2) Two receive SAKs

   3) One of the two receive SAKs at a time for transmission, with the ability to change from one to the other within the time specified in Table 10-1

m) Specify the following parameters for each Cipher Suite implemented

   1) The maximum number of receive SCs supported

   2) The maximum number of receive SAKs

An implementation of a MAC Security Entity (SecY) for which conformance to this standard is claimed shall not

n) Introduce an undetected frame error rate greater than that achievable by preserving the original FCS, as required by 10.4.

o) Implement any Cipher Suite that is additional to those specified in Clause 14 and does not meet all the criteria specified in 14.2, 14.3, and 14.4.1.

p) Support access to MACsec parameters using any version of SNMP prior to v3.

An implementation of a MAC Security Entity (SecY) for which full conformance to this standard is claimed shall not

q) Implement Cipher Suites other than those specified in Clause 14.

NOTE—Conformance with Cipher Suite variance is allowed, as specified in 5.4 and in 14.4.1.

5.4 Optional capabilities

An implementation of a SecY for which conformance to this standard is claimed may

a) Support network management using the MIB specified in Clause 13.

b) Support access to the MIB specified in Clause 13 using SNMP version v3 or higher.

c) Support more than one receive SC.

d) Support more than two receive SAKs.

e) Support Confidentiality Protection using the Default Cipher Suite without a confidentiality offset, as specified in Clause 14.
f) Support Confidentiality Protection using the Default Cipher Suite with a confidentiality offset, as specified in Clause 14.
g) Include Cipher Suites that are specified in Clause 14 in addition to the Default Cipher Suite.

An implementation of a MAC Security Entity (SecY) for which conformance with Cipher Suite variance is claimed may

h) Use Cipher Suites not specified in Clause 14, but meeting the criteria specified in 14.2, 14.3, 14.4.1.

NOTE—The term *capability* is used to describe a set of related detailed provisions of this standard. Each capability can comprise both mandatory provisions, required if implementation of the capability is to be claimed, and optional provisions. Each detailed provision is specified in one or more of the other clauses of this standard. The PICS, described in Annex A (normative), provides a useful checklist of these provisions.

6. Secure provision of the MAC Service

This amendment makes no change to Clause 6 Secure provision of the MAC Service.

7. Principles of secure network operation

Change the note that appears in clause 7.1 Support of the secure MAC Service by an individual LAN as follows:

NOTE—An SC can be required to last for many years without interruption, since interrupting the MAC Service can cause client protocols to re-initialize and recalculate aggregations, spanning trees, and routes (for example). An SC lasts through a succession of SAs, each using a new SAK, to defend against a successful attack on a key while it is still in use. In contrast it is desirable to use a new SAK at periodic intervals to defend against a successful attack on a key while it is still in use. In addition, the MACsec protocol (Clause 8 and Clause 9) only allows a limited number of frames to be protected with a single key unless a Cipher Suite that supports extended packet numbering is used. Since 2^{32} minimum-sized IEEE 802.3 frames can be sent in approximately 5 min at 10 Gb/s, this can force the use of a new SA.

7.1.2 Use of the secure MAC Service by bridges

Change the first paragraph of clause 7.1.2 Secure Channel (SC) as follows:

Each SecY transmits frames conveying secure MAC Service requests on a single SC. Each SC provides unidirectional point-to-multipoint communication, and it can be long lived, persisting through SAK changes. Each SC is identified by a Secure Channel Identifier (SCI) comprising a uniquely allocated 48-bit MAC address concatenated with a 16-bit port number.

8. MAC Security Protocol (MACsec)

<<The editor notes that he has no idea what clause 8.2.6 means.>>

8.1.2 Manageability Requirements

Change the second paragraph of clause 8.1.2 as follows:

<<Only lower 32-bits of PN in frame so frame doesn't vary when using a Cipher Suite with extended packet numbering.>>

8.3 MACsec operation

Change the fourth through seventh paragraphs of clause 8.1 as follows:.

On transmission, the frame is first assigned to an SA (7.1.3), identified locally by its Association Number (AN) (see 7.1.3, 9.6). The AN is used to identify the SAK (7.1.3), and the next PN (3.27, 9.8) for that SA. The AN, the SCI (7.1.2), and the 32 least significant bits of the PN are encoded in the SecTAG (the SCI can be omitted for point-to-point CAs) along with the MACsec EtherType (9.8) and the number of octets in the frame following the SecTAG (SL, 9.7) if less than 48 (8.1.3).

The protection function (14.1) of the Current Cipher Suite is presented with the SAK, the PN and SCI, the destination and source addresses of the frame together with the octets of the SecTAG, and the User Data. It returns the ICV.

On receipt of a MACsec frame, the AN, SCI, PN, and SL field (if present) are extracted from the SecTAG. If ~~(if~~ the CA is point-to-point and the SCI is not present, the value previously communicated by the KaY will be used~~)~~. The AN and SCI are used to assign the frame to an SA, and hence to identify the SAK. If the Current Cipher Suite uses extended packet numbering (a 64-bit PN), the full PN is recovered (as specified in 10.6) using the 32 least significant bits conveyed in the SecTAG and the 32 most significant bits used in a prior successful frame validation.

The validation function of the Current Cipher Suite is presented with the SAK, the PN and SCI, the destination and source addresses of the frame together with the octets of the SecTAG, and the Secure Data and ICV. If the integrity of the frame has been preserved and the User Data can be successfully decoded from the Secure Data, a VALID indication and the octets of the User Data are returned.

9. Encoding of MACsec protocol data units

Change clause 9.3 and Figure 9-2 as follows:

9.3 Security TAG

The Security TAG (SecTAG) is identified by the MACsec EtherType (9.4), and conveys the

a) TAG Control Information (TCI, 9.5)
b) Association Number (AN, 9.6)
c) Short Length (SL, 9.7)
d) Packet Number (PN, 9.8)
e) Optionally encoded Secure Channel Identifier (SCI, 9.9).

The format of the SecTAG is illustrated in Figure 9-2.

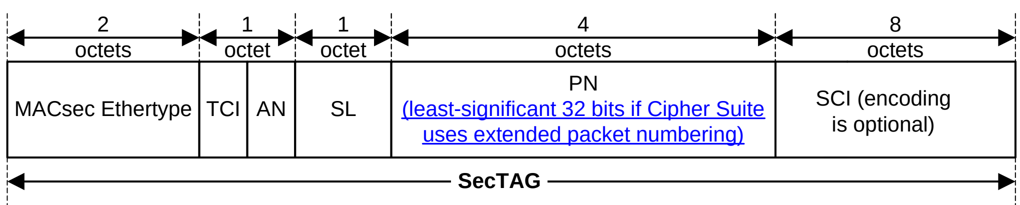


Figure 9-2—SecTAG format

Change clause 9.8 as follows:

9.8 Packet Number (PN)

The 32 least significant bits of the PN ~~is~~ are encoded in octets 5 through 8 of the SecTAG to

a) Provide a unique IV PDU for all MPDUs transmitted using the same SA
b) Support replay protection

NOTE 1—As specified in this clause, the IV used by the default Cipher Suite (GCM-AES-128) comprises the SCI (even if the SCI is not transmitted in the SecTAG) and ~~the~~ a 32-bit PN. Subject to proper unique MAC Address allocation procedures, the SCI is a globally unique identifier for a SecY. To satisfy the IV uniqueness requirements of CTR mode of operation, a fresh key is used before PN values are reused.

NOTE 2—If the Current Cipher Suite provides extended packet numbering, i.e. uses a 64-bit PN, the 32 least significant bits of the PN are conveyed in this SecTAG field and the 32 most significant bits are recovered on receipt as specified in 10.6. The IV used by such a Cipher Suite (e.g. GCM-AES-XPN-128, 14.7) comprises a 32-bit SSCI distributed by key agreement protocol and unique for each SCI within the scope of the CA (and hence within potential users of the same SAK) and the 64-bit non-repeating PN.

9.9 Secure Channel Identifier (SCI)

Change the last paragraph of clause 9.9 as follows:

An explicitly encoded SCI field in the SecTAG is not required on point-to-point links, which are identified by the operPointToPointMAC status parameter of the service provider. In the point-to-point case, the secure association created by the SecY for the peer SecYs, together with the direction of transmission of the secured MPDU, can be used to identify the transmitting SecY and therefore an explicitly encoded SCI is unnecessary. Although the SCI does not have to be repeated in each frame when only two SecYs participate in a CA (see Clause 8, Clause 9, and Clause 10), the SCI (for Cipher Suites using a 32-bit PN) or the SSCI (for Cipher Suites using a 64-bit PN) still forms part of the cryptographic computation.

10. Principles of MAC Security Entity (SecY) operation

Change clause 10.5.2, as follows:

10.5.2 Transmit PN assignment

The frame's PN is set to the value of nextPN for the SA, and nextPN is incremented. If the nextPN variable for the encodingSA is zero (or 2^{32} if the Current Cipher Suite does not support extended packet number, 2^{64} if it does) and the protectFrames control is set MAC_Operational transitions to False for the Controlled Port and frames are neither accepted or delivered. The initial value of nextPN is set by the KaY via the LMI prior to use of the SA, and its current value can be read both while and after the SA is used to transmit frames. The value of nextPN can be read, but not written, by network management.

10.6 Secure frame verification

Change the initial paragraphs of clause 10.6 Secure frame verification, as follows:

For each receive indication from the Receive Demultiplexer, the Secure Frame Verification process

a) Examines the user data for a SecTAG
b) Validates frames with a SecTAG as specified in 9.12
c) Extracts and decodes the SecTAG as specified in 9.3 through 9.9
d) Extracts the User Data and ICV as specified in 9.10 and 9.11
e) Assigns the frame to an SA (10.6.1)
f) Recovers the PN and p~~P~~erforms a preliminary replay check against the last validated PN for the SA (10.6.2)
g) Provides the validation function (14.1, 10.6.3) of the Current Cipher Suite with
   1) The SA Key (SAK)
   2) The SCI for the SC used by the SecY to transmit
   3) The PN
   4) The SecTAG
   5) The sequence of octets that compose the Secure Data
   6) The ICV
h) Receives the following parameters from the Cipher Suite validation operation
   7) A Valid indication, if the integrity check was valid and the User Data could be recovered
   8) The sequence of octets that compose the User Data
i) Updates the replay check (10.6.4)
j) Issues an indication to the Controlled Port with the DA, SA, and priority of the frame as received from the Receive Demultiplexer, and the User Data provided by the validation operation (10.6.5).

If the management control validateFrames is not Strict, frames without a SecTAG are received, counted, and delivered to the Controlled Port; otherwise, they are counted and discarded. If validateFrames is Disabled, cryptographic validation is not applied to tagged frames, but frames whose original service user data can be recovered are delivered. Frames with a SecTAG that has the TCI E bit set but the C bit clear are discarded, as this reserved encoding is used to identify frames with a SecTAG that are not to be delivered to the Controlled Port. Figure 10-5 summarizes the operation of management controls and counters.

Change clause 10.6.2 Preliminary replay check, as follows:

10.6.2 PN recovery and p~~P~~reliminary replay check

If the Current Cipher Suite does not use extended packet numbering, i.e. the PN comprises 32-bits, the value of the PN is that of the lower 32 bits decoded from the SecTAG of the received frame. If extended packet numbering is used, the 32 most significant bits are recovered for each received frame as specified in by applying the assumption that they have remained unchanged since their use in the frame with the lowest acceptable PN (10.6.2) — unless the most significant of the 32 least significant bits of the lowest acceptable PN is set and the corresponding bit of the received PN is not set, in which case the 32 most significant bits of the PN are those of the lowest acceptable PN incremented by one.

NOTE—If a large number of successive frames were to be lost (2^{30}-1, corresponding to approximately 9 seconds of full utilization of a 400 Gb/s link by minimum sized Ethernet frames) subsequent receipt of MACsec frames might fail to establish a correct PN value. MKA, the MACsec Key Agreement protocol specified in IEEE Std 802.1X and its amendments communicates the value of the high order bits periodically to recover from this eventuality.

<<An alternative to the above specification for incrementing the high order bits of the PN would have been to subtract the received bits from the lowest acceptable PN (lower order bits) and perform the high order increment if the answer was more than +0x8000 0000 0000 0000. However it is most likely that dedicated logic will be required for operation at the intended speed, and that operation would require more gates than the test described.>>

If replayProtect control is enabled and the PN of the received frame is less than the lowest acceptable packet number (see 10.6.5) for the SA, the frame is discarded and the InPktsLate counter incremented.

NOTE—If the SC is supported by a network that includes buffering with priority queueing, such as a provider bridged network, delivered frames can be reordered.

10.7 SecY management

Insert the following NOTE after the second paragraph (beginning “Figure 10-6 illustrates the management information ...’) of clause 10.7 SecY management:

NOTE—Figure 10-6 omits parameters specific to extended packet numbering (used by some but not all Cipher Suites (14.7, 14.8)) and not accessible by network management. Specifically: 1. the createReceiveSA(), ReceiveSA(), createTransmitSA(), and TransmitSA() procedures all take an additional SSCI parameter, whose value becomes a parameter of the created SA; 2. the install_key() procedure takes an additional Salt parameter, whose value becomes an inaccessible parameter of the Data_key object. These parameters are specified in 10.7.13, 10.7.21, 10.7.23.

Change clause 10.7.8 Frame verification controls, as follows:

10.7.8 Frame verification controls

Frame verification is subject to the following controls, as specified in 10.6:

a) validateFrames, taking values of Disabled, Check, or Strict, with a default of Strict.
b) replayProtect, True or False, with a default of True.
c) replayWindow, taking values between 0 and 2^{32}–1, with a default of 0.

The validateFrames and replayProtect controls are provided to facilitate deployment. They can be read by management. Each may be written by management, but a conformant implementation shall provide a mechanism to allow write access by network management to be disabled for each parameter individually. If management access is prohibited to any of these parameters, its default value should be used.

If the Current Cipher Suite uses extended packet numbering, i.e. a 64-bit PN, then the maximum value of replayWindow used in the Secure Frame Verification process (10.6) is 2^{30}–1, but any higher value set by network management is retained for possible subsequent use with a different Cipher Suite and will be reported if read by network management. This provision provides compatibility with prior revisions of this standard, though it is unlikely that such a high value of replayWindow would have been used.

Change clauses 10.7.13 and 10.7.14, as follows:

10.7.13 Receive SA creation

A receive SA is created for an existing SC on request from the KaY, with the following parameters:

a) The association number, AN, for the SA
b) nextPN (10.6, 10.6.5)
c) lowestPN, the lowest acceptable PN value for a received frame (10.6, 10.6.2, 10.6.4, 10.6.5)
d) A reference to an SAK that is unchanged for the life of the SA

and, if the Current Cipher Suite uses extended packet numbering (e.g. 14.7, 14.8), the following parameter:

e) an SSCI, unique within all the SecY's (each associated with a KaY, and identified by an SCI) using the SAK, and subsequently available for Cipher Suite protection and validation operations

Frame verification statistics (10.7.9) for the SA are set to zero when the SA is created. Any prior SA with the same AN for the SC is deleted. Creation of the SA fails unless the referenced SAK exists and is installed (i.e., is available for use). A management protocol dependent reference is associated with each SA. This reference allows each SA to be distinguished from any previously created for the same SCI and AN.

10.7.14 Receive SA status

The following parameters can be read, but not directly written, by management:

a) inUse
b) nextPN (10.6, 10.6.5)
c) lowestPN, the lowest acceptable PN value for a received frame (10.6, 10.6.2, 10.6.4, 10.6.5)
d) createdTime, the system time when the SA was created
e) startedTime, the system time when inUse last became True for the SA
f) stoppedTime, the system time when inUse last became False for the SA

If inUse is True, and MAC_Operational is True for the Common Port, the SA can receive frames.

Change clauses 10.7.21 and 10.7.22, as follows:

10.7.21 Transmit SA creation

An SA is created for the transmit SC on request from the KaY, with the following parameters:

a) AN, the association number for the SA
b) nextPN, the initial value of Transmit PN (10.5.2) for the SA
c) confidentiality, True if the SA is to provide confidentiality as well as integrity for transmitted frames
d) A reference to an SAK that is unchanged for the life of the SA

and, if the Current Cipher Suite uses extended packet numbering(e.g. 14.7, 14.8), the following parameter:

e) an SSCI, unique within all the SecY's (each associated with a KaY, and identified by an SCI) using the SAK, and subsequently available for Cipher Suite protection and validation operations.

Frame generation statistics (10.7.18) for the SA are set to zero when the SA is created. Any prior SA with the same AN is deleted. Creation of the SA fails unless the referenced SAK exists and is installed (i.e., is available for use). A management protocol dependent reference is associated with each SA. This reference allows the transmit SA to be distinguished from any previously created with the same AN.

10.7.22 Transmit SA status

The following parameters can be read, but not directly written, by management:

a) inUse
b) nextPN (10.5, 10.5.2)
c) createdTime, the system time when the SA was created
d) startedTime, the system time when inUse last became True for the SA
e) stoppedTime, the system time when inUse last became False for the SA.

If inUse is True, and MAC_Operational is True for the Common Port, the SA can transmit frames.

Change clauses 10.7.26 and 10.7.27, as follows:

10.7.23 SAK creation

An SAK record is created on request from the KaY, with the following parameters:

a) The SAK value
b) A Key Identifier, used by network management to reference the key

and, if the Current Cipher Suite uses extended packet numbering, the following parameter:

c) Salt, a 96-bit parameter subsequently available for Cipher Suite protection and validation operations.

10.7.24 SAK status

The following parameters can be read, but not directly written, by management:

a) transmits, True if the key has been installed for transmission, i.e., can be referenced by a transmit SA
b) receives, True if the key has been installed for reception, i.e., can be referenced by a receive SA
c) createdTime, the system time when the SAK record was created

11. MAC Security in Systems

This amendment makes no changes to Clause 11.

12. MACsec and EPON

This amendment makes no changes to Clause 12.

13. Management protocol

Insert a new clause 13.7 Use of the MIB with extended packet numbering, as follows:

13.7 Use of the MIB with extended packet numbering

Although originally defined prior to the specification of Cipher Suites using extended packet numbering, the MAC Security MIB is applicable both when such Cipher Suites are implemented and when they are not. A conformant implementation with extended packet numbering Cipher Suites also includes the Default Cipher Suite (to provide interoperability) and retention of the existing MIB minimizes any disruption to deployed network management. The MIB accommodates the addition and identification of new Cipher Suites.

The addition of the SSCI (10.7.13, 10.7.21) and Salt (10.7.23) parameters in support of extended packet numbering does not require any addition to the MIB. The Salt parameter has to remain secret (just like an SAK) if its benefits are to be realized, so inclusion in any MIB would be most undesirable. Allocation of the SSCI is a matter for key agreement protocol, and is monitored (if at all) by the management arrangements for that protocol.

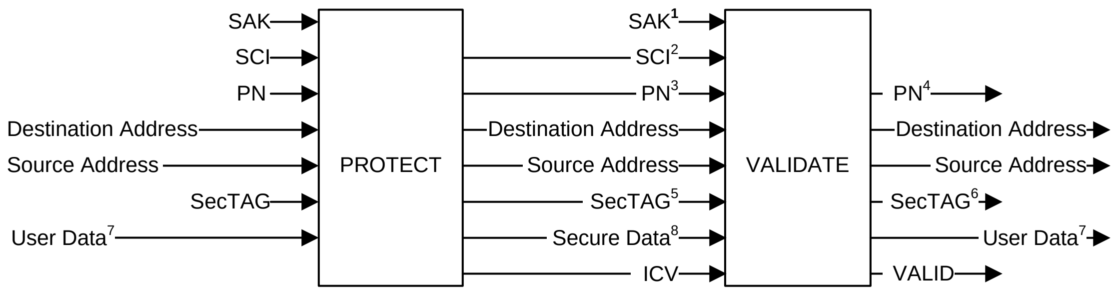
The MIB contains a number of 32-bit statistic counters for each active SA (10.7.14, 10.7.22, 10.7.9). As an active SA is replaced by its successor these statistics are accumulated into a 64-bit counter for the parent SC, and each of the statistics reported by management for an SC comprise the sum of past accumulated values and the active SA values. If the Current Cipher Suite uses a 32-bit PN, none of these 32-bit counters can overflow. If the Current Cipher Suite uses extended packet numbering, each SC statistic is incremented each time a counter for a corresponding SA statistic overflows and wraps. Each of the counters for an SA statistic thus holds the lower 32-bits of the value accumulated since the creation of the SA. The createdTime for the SA remains unchanged when and if any counter wraps. Similarly the 32-bit SA object for the nextPN reports the lower 32-bits of that parameter. The relevant MIB objects are:

```
secyTxSANextPN                Unsigned32
secyRxSANextPN                Unsigned32
secyTxSAStatsProtectedPkts    Counter32
secyTxSAStatsEncryptedPkts    Counter32
secyRxSAStatsUnusedSAPkts     Counter32
secyRxSAStatsNoUsingSAPkts    Counter32
secyRxSAStatsNotValidPkts     Counter32
secyRxSAStatsInvalidPkts      Counter32
secyRxSAStatsOKPkts           Counter32
```

14. Cipher Suites

14.1 Cipher Suite use

Change footnote2 and footnote 3 in Figure 14-1 as follows:



[1] The SAK to be used on receipt of the frame is identified by the SCI and the AN.

[2] The SCI is extracted from the SCI field of the SecTAG if present. A value conveyed by key agreement (point-to-point only) is used otherwise.
In the GCM-AES-128 and GCM-AES-256 Cipher Suites (14.5, 14.6), the SCI is always included in the IV parameter whether included in the SecTAG or not (and thus always contributes to the ICV). However the Cipher Suite parameter A includes the SCI if and only if the SCI is included in the SecTAG.
In the GCM-AES-XPN-128 and GCM-AES-XPN-256 Cipher Suites (14.7, 14.8), the {SCI, SAK} tuple (or equivalently the SA) identifies the SSCI (conveyed by key agreement) that is included in the IV parameter, and the Cipher Suite parameter A includes the SCI if and only if the SCI is included in the SecTAG.

[3] The 32 least significant bits of the PN are ~~is~~ conveyed in the SecTAG

[4] The validated PN can be used for replay protection.

[5] All the transmitted octets of the SecTAG are protected, including the optional SCI field if present

[6] The validated received SecTAG contains bits of the TCI, and optionally the SCI, these can be used for service multiplexing (11.7).

[7] The length, in octets, of the User Data is conveyed by the User Data parameter, and is protected by Cipher Suite operation.

[8] The length, in octets, of the Secure Data is conveyed by the MACsec frame, unless it is short, when it is conveyed by the SL parameter in the SecTAG TCI

Figure 14-1—Cipher Suite Protect and Validate operations

Change the fourth paragraph of clause 14.1 and add a NOTE as follows:

The PN (Packet Number, 3.27, 8.3) is a ~~32-bit~~ number that is never zero, is incremented each time a protect request is made for a given SCI, and is never repeated for an SCI unless the SAK is changed. The size of the PN depends on the Cipher Suite, and is 32-bits unless otherwise specified. Cipher suites that provide extended packet numbering use a 64-bit PN. Irrespective of the size of the PN, only the least significant 32-bits are conveyed in the SecTAG. If extended packet numbering is used, the most significant 32-bits are recovered for each received frame as specified in 10.6.2.

14.4 Cipher Suite conformance

Change Table 14-1 as follows:

Table 14-1—MACsec Cipher Suites

Cipher Suite # Identifier	Cipher Suite Name	Services provided		Mandatory/Optional	Defining Clause
		Integrity without confidentiality	Integrity and confidentiality		
00-80-C2-00-01-00-00-01	GCM–AES–128	Yes	Yes	Mandatory	14.5
00-80-C2-00-01-00-00-02	GCM-AES-256	Yes	Yes	Optional	14.6
00-80-C2-00-01-00-00-03	GCM–AES–XPN-128	Yes	Yes	Optional	14.7
00-80-C2-00-01-00-00-04	GCM-AES-XPN-256	Yes	Yes	Optional	14.8

Change clause 14.6 as follows:

14.6 GCM–AES–256

GCM-AES-256 uses the Galois/Counter Mode of operation with the AES-256 symmetric block cipher, as specified in this clause by reference to the terms *K, IV, A, P, C, T* used in NIST SP 800-38D.

K is the 256 bit SAK. The 64 most significant bits of the 96-bit *IV* are the octets of the SCI, encoded as a binary number (9.1). The 32 least significant bits of the 96-bit *IV* are the octets of the PN, encoded as a binary number (9.1). *T* is the ICV, and is 128 bits long. When the bit-strings *A*, *P*, and *C* are specified in terms of octet strings, earlier octets compose earlier bits, and more significant bits in each octet are earlier.

NOTE—The bit strings obtained by transforming MAC Address and data octets using these rules do not correspond to 802.3 'wire order' for frame transmission.

When ~~the Default~~ this Cipher Suite is used for Integrity Protection

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and User Data concatenated in that order.
— *P* is null.
— The Secure Data is the octets of the User Data, without modification.

When ~~the Default~~ this Cipher Suite is used for Confidentiality Protection without a confidentiality offset

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG concatenated in that order.
— *P* is the octets of the User Data.
— The Secure Data is *C*.

When ~~the Default~~ this Cipher Suite is used for Confidentiality Protection with a confidentiality offset

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and the first confidentialityOffset (10.7.24) octets of the User Data concatenated in that order.
— *P* is the remaining octets of the User Data.
— The Secure Data is the first confidentialityOffset octets of the User Data concatenated with *C*, in that order.

Insert clause 14.7 as follows:

14.7 GCM–AES–XPN-128

Each instance of the GCM-AES-XPN-128 Cipher Suite, i.e. the protection and validation capabilities created for a given SAK at the request of the KaY (10.7.26, Figure 10-6) maintains an instance of the following parameter as specified in 10.7.23:

a) Salt, a 96-bit value distributed by key agreement protocol to all members of the CA.

The MACsec Key Agreement (MKA) protocol specified in IEEE 802.1X-2010 does not include explicit parameters for distributing the Salt (applicable to all SAs using a given SAK) or the SSCI (applicable to a given SA, using a given SAK) explicitly. Each KaY computes these parameters from the MKA protocol information as follows. The 64 least-significant bits of the Salt comprise the SCI of the MKA Key Server, and the 32 most significant bits of the Salt comprise the value obtain by the exclusive-or of the 32 most significant and the 32 least significant bits of that SCI. The KaY with numerically greatest SCI uses the SSCI value 0x0001, the KaY with the next to the greatest SCI uses the SSCI value 0x0002, and so on.

NOTE 1—This procedure does not ensure that the Salt is secret. Readers of this standard are encouraged to consult the latest revision of 802.1X and its amendments.

NOTE 2—MKA guarantees that each KaY that receives a given SAK has a unique SCI, and these SCIs are present in every MKPDU that conveys a (key-wrapped) SAK.

GCM-AES-XPN-128 uses the Galois/Counter Mode of operation with the AES-128 symmetric block cipher, as specified in this clause by reference to the terms *K, IV, A, P, C, T* used in NIST SP 800-38D.

K is the 128 bit SAK. The 32 most significant bits of the 96-bit *IV* are the octets of the SSCI, encoded as a binary number (9.1) and exclusive-or’d with the 32 most significant bits of the Salt. The 64 least significant bits of the 96-bit *IV* are the octets of the PN, encoded as a binary number (9.1) and exclusive-or’d with the 64 least significant bits of the Salt. *T* is the ICV, and is 128 bits long. When the bit-strings *A*, *P*, and *C* are specified in terms of octet strings, earlier octets compose earlier bits, and more significant bits in each octet are earlier.

NOTE 3—The bit strings obtained by transforming MAC Address and data octets using these rules do not correspond to 802.3 'wire order' for frame transmission.

When this Cipher Suite is used for Integrity Protection

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and User Data concatenated in that order.
— *P* is null.
— The Secure Data is the octets of the User Data, without modification.

When this Cipher Suite is used for Confidentiality Protection without a confidentiality offset

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG concatenated in that order.
— *P* is the octets of the User Data.
— The Secure Data is *C*.

This Cipher Suite does not provide Confidentiality Protection with a confidentiality offset.

Insert clause 14.8 as follows:

14.8 GCM–AES–XPN-256

Each instance of the GCM-AES-XPN-256 Cipher Suite, i.e. the protection and validation capabilities created for a given SAK at the request of the KaY (10.7.26, Figure 10-6) maintains an instance of the following parameter as specified in 10.7.23:

a) Salt, a 96-bit value distributed by key agreement protocol to all members of the CA.

The MACsec Key Agreement (MKA) protocol specified in IEEE 802.1X-2010 does not include explicit parameters for distributing the Salt (applicable to all SAs using a given SAK) or the SSCI (applicable to a given SA, using a given SAK) explicitly. Each KaY computes these parameters from the MKA protocol information as follows. The 64 least-significant bits of the Salt comprise the SCI of the MKA Key Server, and the 32 most significant bits of the Salt comprise the value obtain by the exclusive-or of the 32 most significant and the 32 least significant bits of that SCI. The KaY with numerically greatest SCI uses the SSCI value 0x0001, the KaY with the next to the greatest SCI uses the SSCI value 0x0002, and so on.

NOTE 1—This procedure does not ensure that the Salt is secret. Readers of this standard are encouraged to consult the latest revision of 802.1X and its amendments.

NOTE 2—MKA guarantees that each KaY that receives a given SAK has a unique SCI, and these SCIs are present in every MKPDU that conveys a (key-wrapped) SAK.

GCM-AES-XPN-256 uses the Galois/Counter Mode of operation with the AES-256 symmetric block cipher, as specified in this clause by reference to the terms *K, IV, A, P, C, T* used in NIST SP 800-38D.

K is the 256 bit SAK. The 32 most significant bits of the 96-bit *IV* are the octets of the SSCI, encoded as a binary number (9.1) and exclusive-or'd with the 32 most significant bits of the Salt. The 64 least significant bits of the 96-bit *IV* are the octets of the PN, encoded as a binary number (9.1) and exclusive-or'd with the 64 least significant bits of the Salt. *T* is the ICV, and is 128 bits long. When the bit-strings *A*, *P*, and *C* are specified in terms of octet strings, earlier octets compose earlier bits, and more significant bits in each octet are earlier.

NOTE 3—The bit strings obtained by transforming MAC Address and data octets using these rules do not correspond to 802.3 'wire order' for frame transmission.

When this Cipher Suite is used for Integrity Protection

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG and User Data concatenated in that order.
— *P* is null.
— The Secure Data is the octets of the User Data, without modification.

When this Cipher Suite is used for Confidentiality Protection without a confidentiality offset

— *A* is the Destination MAC Address, Source MAC Address, and the octets of the SecTAG concatenated in that order.
— *P* is the octets of the User Data.
— The Secure Data is *C*.

This Cipher Suite does not provide Confidentiality Protection with a confidentiality offset.

Annex A (normative)

(normative)

PICS Proforma

This amendment makes no changes to Annex A, PICS Proforma.

Annex B (informative)

(informative)

Bibliography

Change the text of this clause as follows, updating cross-references as necessary.

<<References to IP related uses of GCM that use 96-bit IV with 64-bit PNs (or equivalent) may be added, if suitable. The following text is that of the Bibliography after applying the 802.1AEbn amendment, with the correction that the later duplicated an entry in the Bibliography.>>

[B1] Fowler, M., "UML Distilled: A Brief Guide to the Standard Object Modeling Language, Third Edition," Pearson Education Inc., Boston, 2004, ISBN 0-321-19368-7.

[B2] IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms*, Seventh Edition.

[B3] IETF RFC 2279, UTF-8, a Transformation format of ISO 10646, Yergeau, F., January 1998.

[B4] IETF RFC 2406, IP Encapsulating Security Payload (ESP), Kent, S., Atkinson, R., November 1998.

[B5] IETF RFC 2737, Entity MIB (Version 2), McCloghrie, K., Bierman, A., December 1999.

[B6] IETF RFC 3232, Assigned Numbers: RFC 1700 is Replaced by an On-line Database, Reynolds, J., January 2002.

[B7] IETF RFC 3410, Introduction and Applicability Statements for Internet-Standard Management Framework, Case, J., Mundy, R., Partain, D., and Stewart, B., December 2002.

[B8] IETF RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Manage-ment Frameworks, Harrington, D., Presuhn, R., and Wijnen, B., December 2002.

[B10] IETF RFC 5116, An Interface and Algorithms for Authenticated Encryption, McGrew, D., January 2008.

[B11] ISO 6937-2: 1983, Information processing—Coded character sets for text communication—Part 2: Latin alphabetic and non-alphabetic graphic characters.[1]

[B12] ISO/IEC TR 11802-2: 1997, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Technical reports and guidelines—Part 2: Standard Group MAC addresses.

[B13] The Galois/Counter Mode of Operation (GCM), David A. McGrew and J. Viega. May 31, 2005.[2]

[B14] The Security and Performance of the Galois/Counter Mode (GCM) of Operation. D. McGrew and J. Viega. Proceedings of INDOCRYPT '04, Springer-Verlag, 2004. [3]

[1]ISO and ISO/IEC documents are available from the ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

[2]A prior revision of this document was the normative reference for GCM in IEEE Std 802.1AE-2006, but has been superseded by NIST SP 800-38D for that purpose. It does contain additional background information, and can be downloaded from http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-revised-spec.pdf

[3]Available from the IACR Cryptology ePrint Archive: Report 2004/193, http://eprint.iacr.org/2004/193

~~[B15] McGrew, D. A., Viega, J., "The Security and Performance of the Galois/Counter Mode (GCM) of Operation (Full Version), http://eprint.iacr.org/2004/193.pdf.~~

Annex C (informative)

(informative)

MACsec Test Vectors

<<The results for the GCM-AES-XPN-128 and GCM-AES-XPN-256 test vectors have yet to be added, Place holders for the hexadecimal representation of intermediate vales and results are shown as '??'.>>

Change the third paragraph of the initial text of this Annex, as follows:

Test cases are provided for both the Default Cipher Suite (GCM-AES-128, 14.5), ~~and~~ GCM-AES-256 (14.6), GCM-AES-XPN-256 (14.7), and GCM-AES-XPN-256 (14.8). The notation used in this Annex is that specified in Clause 14 (Cipher Suites) and NIST SP 800-38D. Fields in the MACsec header are specified in Clause 9. Summaries of the computation and intermediate outputs are provided.

C.1 Integrity protection (54-octet frame)

Change the initial paragraphs and tables of clause C.1 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-1. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-1—Unprotected frame (example)

Field	Value
MAC DA	D6 09 B1 F0 56 63
MAC SA	7A 0D 46 DF 99 8D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 01

The MAC Security TAG (SecTAG) comprises the MACsec EtherType, the TCI, the AN, the SL, the PN (32 least significant bits for Cipher Suites using extended packet numbering), and the (optional) SCI. The PN differs for each protected frame transmitted with any given SAK (*K*) and has been arbitrarily chosen (for this and in other examples) as have the other parameter values. The fields of the protected frame are shown (in the order transmitted) in Table C-2.

Table C-2—Integrity protected frame (example)

Field	Value
MAC DA	D6 09 B1 F0 56 63
MAC SA	7A 0D 46 DF 99 8D
MACsec EtherType	88 E5
TCI and AN	22
SL	2A
PN	B2 C2 84 65
SCI	12 15 35 24 C0 89 5E 81
Secure Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 01
ICV	Cipher Suite and Key (SAK) dependent (see Table C-3 ~~and~~, Table C-4, Table C-5, and Table C-6)

~~The GCM parameter *A*, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The SCI and the PN are concatenated (in that order) to form the 96-bit *IV* used by GCM. The computed GCM parameter *T* is the ICV.~~

C.1.1 GCM-AES-128 (54-octet frame integrity protection)

Change clause C.1.1 as follows:

Table C-3 specifies an arbitrary 128-bit key (SAK), and the ICV generated by the GCM-AES-128 Cipher Suite when that key is used in conjunction with the frame field data of Table C-2. The GCM parameter A, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The SCI and the PN are concatenated (in that order) to form the 96-bit IV used by GCM. The computed GCM parameter T is the ICV. Details of the computation follow the table.

Table C-3—GCM-AES-128 Key and calculated ICV (example)

Field	Value
Key (SAK)	AD7A2BD03EAC835A6F620FDCB506B345
ICV	F0 94 78 A9 B0 90 07 D0 6F 46 E9 B6 A1 DA 25 DD

```
key size = 128 bits
P:     0 bits
A:     560 bits
IV:    96 bits
ICV:   128 bits
K:     AD7A2BD03EAC835A6F620FDCB506B345
P:
A:     D609B1F056637A0D46DF998D88E5222A
       B2C2846512153524C0895E8108000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       313233340001
IV:    12153524C0895E81B2C28465
GCM-AES Authentication
H:     73A23D80121DE2D5A850253FCF43120E
Y[0]:  12153524C0895E81B2C2846500000001
E(K,Y[0]): EB4E051CB548A6B5490F6F11A27CB7D0
X[1]:  6B0BE68D67C6EE03EF7998E399C01CA4
X[2]:  5AABADF6D7806EC0CCCB028441197B22
X[3]:  FE072BFE2811A68AD7FDB0687192D293
X[4]:  A47252D1A7E09B49FB356E435DBB4CD0
X[5]:  18EBF4C65CE89BF69EFB4981CEE13DB9
GHASH(H,A,C): 1BDA7DB505D8A165264986A703A6920D
C:
T:     F09478A9B09007D06F46E9B6A1DA25DD
```

C.1.2 GCM-AES-256 (54-octet frame integrity protection)

Change clause C.1.2 as follows:

Table C-4 specifies an arbitrary 256-bit key (SAK), and the ICV generated by the GCM-AES-256 Cipher Suite when that key is used in conjunction with the frame field data of Table C-2. The GCM parameter A, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The SCI and the PN are concatenated (in that order) to form the 96-bit IV used by GCM. The computed GCM parameter T is the ICV. Details of the computation follow the table.

Table C-4—GCM-AES-256 Key and calculated ICV (example)

Field	Value
Key (SAK)	E3C08A8F06C6E3AD95A70557B23F7548 3CE33021A9C72B7025666204C69C0B72
ICV	2F 0B C5 AF 40 9E 06 D6 09 EA 8B 7D 0F A5 EA 50

```
key size = 256 bits
P:      0 bits
A:      560 bits
IV:     96 bits
ICV:    128 bits
K:      E3C08A8F06C6E3AD95A70557B23F7548
        3CE33021A9C72B7025666204C69C0B72
P:
A:      D609B1F056637A0D46DF998D88E5222A
        B2C2846512153524C0895E8108000F10
        1112131415161718191A1B1C1D1E1F20
        2122232425262728292A2B2C2D2E2F30
        313233340001
IV:     12153524C0895E81B2C28465
GCM-AES Authentication
H:      286D73994EA0BA3CFD1F52BF06A8ACF2
Y[0]:   12153524C0895E81B2C2846500000001
E(K,Y[0]): 714D54FDCFCEE37D5729CDDAB383A016
X[1]:   BA7C26F578254853CF321281A48317CA
X[2]:   2D0DF59AE78E84ED64C3F85068CD9863
X[3]:   702DE0382ABF4D42DD62B8F115124219
X[4]: DAED65979342F0D155BFDFE362132078
X[5]: 9AB4AFD6344654B2CD23977E41AA18B3
GHASH(H,A,C): 5E4691528F50E5AB5EC346A7BC264A46
C:
T: 2F0BC5AF409E06D609EA8B7D0FA5EA50
```

Insert a new clause C.1.3 as follows:

C.1.3 GCM-AES-XPN-128 (54-octet frame integrity protection)

Table C-5 specifies an arbitrary value for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 128-bit key (SAK), with the ICV generated by the GCM-AES-XPN-128 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-2. The GCM parameter A, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The 32 most significant bits of the 96-bit IV are the octets of the SCI, encoded as a binary number (9.1) and exclusive-or'd with the 32 most significant bits of the Salt. The 64 least significant bits of the 96-bit IV are the octets of the PN, encoded as a binary number (9.1) and exclusive-or'd with the 64 least significant bits of the Salt. The computed GCM parameter T is the ICV. Details of the computation follow the table.

Table C-5—GCM-AES-XPN-128 Key and calculated ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	AD7A2BD03EAC835A6F620FDCB506B345
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits
P:     0 bits
A:     560 bits
IV:    96 bits
ICV:   128 bits
K:     AD7A2BD03EAC835A6F620FDCB506B345
P:
A:     D609B1F056637A0D46DF998D88E5222A
       B2C2846512153524C0895E8108000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       313233340001
IV:    ????????????????????????
GCM-AES Authentication
H:     ????????????????????????????????
Y[0]:  ????????????????????????????????
E(K,Y[0]): ????????????????????????????????
X[1]:  ????????????????????????????????
X[2]:  ????????????????????????????????
X[3]:  ????????????????????????????????
X[4]:  ????????????????????????????????
X[5]:  ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:
T:     ????????????????????????????????
```

Insert a new clause C.1.4 as follows:

C.1.4 GCM-AES-XPN-256 (54-octet frame integrity protection)

Table C-6 specifies an arbitrary value for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 256-bit key (SAK), with the ICV generated by the GCM-AES-XPN-256 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-2. The GCM parameter A, the additional data to be authenticated, is formed by concatenating the MAC DA, the MAC SA, the SecTAG, and the User Data. This input is then processed through the authentication only operation of the GCM module. The 32 most significant bits of the 96-bit IV are the octets of the SCI, encoded as a binary number (9.1) and exclusive-or’d with the 32 most significant bits of the Salt. The 64 least significant bits of the 96-bit IV are the octets of the PN, encoded as a binary number (9.1) and exclusive-or’d with the 64 least significant bits of the Salt. The computed GCM parameter T is the ICV. Details of the computation follow the table.

Table C-6—GCM-AES-XPN-256 Key and calculated ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	E3C08A8F06C6E3AD95A70557B23F7548 3CE33021A9C72B7025666204C69C0B72
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 256 bits
P:     0 bits
A:     560 bits
IV:    96 bits
ICV:   128 bits
K:     E3C08A8F06C6E3AD95A70557B23F7548
       3CE33021A9C72B7025666204C69C0B72
P:
A:     D609B1F056637A0D46DF998D88E5222A
       B2C2846512153524C0895E8108000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       313233340001
IV:    ????????????????????????
GCM-AES Authentication
H:     ????????????????????????????????
Y[0]:  ????????????????????????????????
E(K,Y[0]): ????????????????????????????????
X[1]:  ????????????????????????????????
X[2]:  ????????????????????????????????
X[3]:  ????????????????????????????????
X[4]:  ????????????????????????????????
X[5]:  ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:
T:     ????????????????????????????????
```

C.2 Integrity protection (60-octet frame)

Change the initial paragraphs and tables of clause C.2 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-7. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-7—Unprotected frame (example)

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 03

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, the PN. In this example the optional SCI has been omitted. The fields of the protected frame are shown (in the order transmitted) in Table C-8.

Table C-8—Integrity protected frame (example)

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
MACsec EtherType	88 E5
TCI and AN	40
SL	00
PN	76 D4 57 ED
Secure Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 03
ICV	Cipher Suite and Key (SAK) dependent (see ~~Table C-7 and Table C-8~~ Table C-9, Table C-10, Table C-11, and Table C-12)

Insert a new clause C.2.3 as follows, renumbering subsequent tables as required:

C.2.3 GCM-AES-XPN-128 (60-octet frame integrity protection)

Table C-11 specifies arbitrary values for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), 96-bit Salt, and 128-bit key (SAK), with the ICV generated by the GCM-AES-XPN-128 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-7.

Table C-11—GCM-AES-XPN-128 Key and calculated ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	071B113B0CA743FECCCF3D051F737382
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits
P:     0 bits
A:     544 bits
IV:    96 bits
ICV:   128 bits
K:     071B113B0CA743FECCCF3D051F737382
P:
A:     E20106D7CD0DF0761E8DCD3D88E54000
       76D457ED08000F101112131415161718
       191A1B1C1D1E1F202122232425262728
       292A2B2C2D2E2F303132333435363738
       393A0003
IV:    ????????????????????????
GCM-AES Authentication
H:     ????????????????????????????????
Y[0]:  ????????????????????????????????
E(K,Y[0]): ????????????????????????????????
X[1]:  ????????????????????????????????
X[2]:  ????????????????????????????????
X[3]:  ????????????????????????????????
X[4]:  ????????????????????????????????
X[5]:  ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:
T:     ????????????????????????????????
```

Insert a new clause C.2.4 as follows:

C.2.4 GCM-AES-XPN-256 (60-octet frame integrity protection)

Table C-12 specifies arbitrary values for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a \96-bit Salt, and 256-bit key (SAK), with the ICV generated by the GCM-AES-XPN-256 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-7.

Table C-12—GCM-AES-XPN-256 Key and calculated ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	691D3EE909D7F54167FD1CA0B5D76908 1F2BDE1AEE655FDBAB80BD5295AE6BE7
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 256 bits
P:     0 bits
A:     544 bits
IV:    96 bits
ICV:   128 bits

K:     691D3EE909D7F54167FD1CA0B5D76908
       1F2BDE1AEE655FDBAB80BD5295AE6BE7

P:

A:     E20106D7CD0DF0761E8DCD3D88E54000
       76D457ED08000F101112131415161718
       191A1B1C1D1E1F202122232425262728
       292A2B2C2D2E2F303132333435363738
       393A0003

IV:    ????????????????????????

GCM-AES Authentication
H:     ????????????????????????????????
Y[0]:  ????????????????????????????????
E(K,Y[0]): ????????????????????????????????
X[1]:  ????????????????????????????????
X[2]:  ????????????????????????????????
X[3]:  ????????????????????????????????
X[4]: ????????????????????????????????
X[5]: ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????

C:

T: ????????????????????????????????
```

C.3 Integrity protection (65-octet frame)

Change the initial paragraphs and tables of clause C.3 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-13. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-13—Unprotected frame (example)

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 00 05

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, the PN, and the (optional) SCI. The fields of the protected frame are shown (in the order transmitted) in Table C-14.

Table C-14—Integrity protected frame (example)

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
MACsec EtherType	88 E5
TCI and AN	23
SL	00
PN	89 32 D6 12
SCI	7C FD E9 F9 E3 37 24 C6
Secure Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 00 05
ICV	(see ~~Table C-11 and Table C-12~~ Table C-15, Table C-16, Table C-17, and Table C-18)

C.3.3 GCM-AES-XPN-128 (65-octet frame integrity protection)

Table C-17 specifies arbitrary values for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), 96-bit Salt, and 128-bit key (SAK), with the ICV generated by the GCM-AES-XPN-128 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-13.

Table C-17—GCM-AES-XPN-128 Key and calculated ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	013FE00B5F11BE7F866D0CBBC55A7A90
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits
P:     0 bits
A:     648 bits
IV:    96 bits
ICV:   128 bits
K:     013FE00B5F11BE7F866D0CBBC55A7A90
P:
A:     84C5D513D2AAF6E5BBD2727788E52300
       8932D6127CFDE9F9E33724C608000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       3132333435363738393A3B3C3D3E3F00
       05
IV:    ????????????????????????
GCM-AES Authentication
H:     ????????????????????????????????
Y[0]:  ????????????????????????????????
E(K,Y[0]): ????????????????????????????????
X[1]:  ????????????????????????????????
X[2]:  ????????????????????????????????
X[3]:  ????????????????????????????????
X[4]:  ????????????????????????????????
X[5]:  ????????????????????????????????
X[6]:  ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:
T:     ????????????????????????????????
```

C.3.4 GCM-AES-XPN-256 (65-octet frame integrity protection)

Table C-18 specifies arbitrary values for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a \96-bit Salt, and 256-bit key (SAK), with the ICV generated by the GCM-AES-XPN-256 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-13.

Table C-18—GCM-AES-XPN-256 Key and calculated ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	83C093B58DE7FFE1C0DA926AC43FB360 9AC1C80FEE1B624497EF942E2F79A823
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 256 bits
P:     0 bits
A:     648 bits
IV:    96 bits
ICV:   128 bits
K:     83C093B58DE7FFE1C0DA926AC43FB360
       9AC1C80FEE1B624497EF942E2F79A823
P:
A:     84C5D513D2AAF6E5BBD2727788E52300
       8932D6127CFDE9F9E33724C608000F10
       1112131415161718191A1B1C1D1E1F20
       2122232425262728292A2B2C2D2E2F30
       3132333435363738393A3B3C3D3E3F00
       05
IV:    ????????????????????????
GCM-AES Authentication
H:     ????????????????????????????????
Y[0]:  ????????????????????????????????
E(K,Y[0]): ????????????????????????????????
X[1]:  ????????????????????????????????
X[2]:  ????????????????????????????????
X[3]:  ????????????????????????????????
X[4]: ????????????????????????????????
X[5]: ????????????????????????????????
X[6]:  ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:
T: ????????????????????????????????
```

C.4 Integrity protection (79-octet frame)

Change the initial paragraphs and tables of clause C.4 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-19. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-19—Unprotected frame (example)

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 00 07

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, and the PN. In this example the optional SCI has been omitted. The fields of the protected frame are shown (in the order transmitted) in Table C-20.

Table C-20—Integrity protected frame (example)

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
MACsec EtherType	88 E5
TCI and AN	41
SL	00
PN	2E 58 49 5C
Secure Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 00 07
ICV	(see ~~Table C-15 and Table C-16~~ Table C-21, Table C-22, Table C-23, and Table C-24)

C.4.3 GCM-AES-XPN-128 (79-octet frame integrity protection)

Table C-23 specifies arbitrary values for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), 96-bit Salt, and 128-bit key (SAK), with the ICV generated by the GCM-AES-XPN-128 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-19.

Table C-23—GCM-AES-XPN-128 Key and calculated ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	88EE087FD95DA9FBF6725AA9D757B0CD
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits
P:     0 bits
A:     696 bits
IV:    96 bits
ICV:   128 bits
K:     88EE087FD95DA9FBF6725AA9D757B0CD
P:
A:     68F2E77696CE7AE8E2CA4EC588E54100
       2E58495C08000F101112131415161718
       191A1B1C1D1E1F202122232425262728
       292A2B2C2D2E2F303132333435363738
       393A3B3C3D3E3F404142434445464748
       494A4B4C4D0007
IV:    ????????????????????????
GCM-AES Authentication
H:     ????????????????????????????????
Y[0]:  ????????????????????????????????
E(K,Y[0]): ????????????????????????????????
X[1]:  ????????????????????????????????
X[2]:  ????????????????????????????????
X[3]:  ????????????????????????????????
X[4]:  ????????????????????????????????
X[5]:  ????????????????????????????????
X[6]:  ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:
T:     ????????????????????????????????
```

C.4.4 GCM-AES-XPN-256 (79-octet frame integrity protection)

Table C-24 specifies arbitrary values for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 256-bit key (SAK), with the ICV generated by the GCM-AES-XPN-256 Cipher Suite when that key is used in conjunction with the foregoing and the frame field data of Table C-19.

Table C-24—GCM-AES-XPN-256 Key and calculated ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	4C973DBC7364621674F8B5B89E5C1551 1FCED9216490FB1C1A2CAA0FFE0407E5
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 256 bits
P:     0 bits
A:     696 bits
IV:    96 bits
ICV:   128 bits
K:     4C973DBC7364621674F8B5B89E5C1551
       1FCED9216490FB1C1A2CAA0FFE0407E5
P:
A:     68F2E77696CE7AE8E2CA4EC588E54100
       2E58495C08000F101112131415161718
       191A1B1C1D1E1F202122232425262728
       292A2B2C2D2E2F303132333435363738
       393A3B3C3D3E3F404142434445464748
       494A4B4C4D0007
IV:    ????????????????????????
GCM-AES Authentication
H:     ????????????????????????????????
Y[0]:  ????????????????????????????????
E(K,Y[0]): ????????????????????????????????
X[1]:  ????????????????????????????????
X[2]:  ????????????????????????????????
X[3]:  ????????????????????????????????
X[4]: ????????????????????????????????
X[5]: ????????????????????????????????
X[6]:  ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:
T: ????????????????????????????????
```

C.5 Confidentiality protection (54-octet frame)

Change the initial paragraphs and tables of clause C.5 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-25. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-25—Unprotected frame (example)

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 00 04

The MAC Security TAG (SecTAG) comprises the MACsec EtherType, the TCI, the AN, the SL, and the PN. In this example the optional SCI has been omitted. The fields of the protected frame are shown (in the order transmitted) in Table C-26.

Table C-26—Confidentiality protected frame (example)

Field	Value
MAC DA	E2 01 06 D7 CD 0D
MAC SA	F0 76 1E 8D CD 3D
MACsec EtherType	88 E5
TCI and AN	4C
SL	2A
PN	76 D4 57 ED
Secure Data	Cipher Suite and Key (SAK) dependent (see ~~Table C-19 and Table C-20~~ Table C-27, Table C-28, Table C-29, and Table C-30)
ICV	Cipher Suite and Key (SAK) dependent (see ~~Table C-19 and Table C-20~~ Table C-27, Table C-28, Table C-29, and Table C-30)

~~The GCM parameter *P*, the data to be encrypted, is the User Data. The additional data *A* to be authenticated is formed by concatenating the MAC DA, the MAC SA, and the SecTAG. The SCI and the PN are concatenated (in that order) to form the 96-bit *IV* used by GCM. The computed GCM parameter *T* is the ICV.~~

C.5.1 GCM-AES-128 (54-octet frame confidentiality protection)

Table C-27 specifies an arbitrary 128-bit key (SAK), the Secure Data, and the ICV generated by the GCM-AES-128 Cipher Suite when that key is used in conjunction with the frame field data of Table C-25. The GCM parameter *P*, the data to be encrypted, is the User Data. The additional data *A* to be authenticated is formed by concatenating the MAC DA, the MAC SA, and the SecTAG. The SCI and the PN are concatenated (in that order) to form the 96-bit *IV* used by GCM. The computed GCM parameter *T* is the ICV. Details of the computation follow the table.

Table C-27—GCM-AES-128 Key, Secure Data, and ICV (example)

Field	Value
Key (SAK)	071B113B0CA743FECCCF3D051F737382
Secure Data	13 B4 C7 2B 38 9D C5 01 8E 72 A1 71 DD 85 A5 D3 75 22 74 D3 A0 19 FB CA ED 09 A4 25 CD 9B 2E 1C 9B 72 EE E7 C9 DE 7D 52 B3 F3
ICV	D6 A5 28 4F 4A 6D 3F E2 2A 5D 6C 2B 96 04 94 C3

```
key size = 128 bits
P:     336 bits
A:     160 bits
IV:    96 bits
ICV:   128 bits
K:     071B113B0CA743FECCCF3D051F737382
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F30313233340004
A:     E20106D7CD0DF0761E8DCD3D88E54C2A
       76D457ED
IV:    F0761E8DCD3D000176D457ED
GCM-AES Encryption
H:            E4E01725D724C1215C7309AD34539257
Y[0]:         F0761E8DCD3D000176D457ED00000001
E(K,Y[0]):    FC25539100959B80FE3ABED435E54CAB
Y[1]:         F0761E8DCD3D000176D457ED00000002
E(K,Y[1]):    1BB4C83B298FD6159B64B669C49FBECF
C[1]:         13B4C72B389DC5018E72A171DD85A5D3
Y[2]:         F0761E8DCD3D000176D457ED00000003
E(K,Y[2]):    683C6BF3813BD8EEC82F830DE4B10530
C[2]:         752274D3A019FBCAED09A425CD9B2E1C
Y[3]:         F0761E8DCD3D000176D457ED00000004
E(K,Y[3]):    B65CC1D7F8EC4E66B3F7182C2E358591
C[3]:         9B72EEE7C9DE7D52B3F3
X[1]:         A0AE6DFAE25C0AE80E9A1AAC0D5123D3
X[2]:         EAEA2A767986B7D5B9E6ED37A3CBC63B
X[3]:         8809F1263C02DC9BD09FDF0F34575BA6
X[4]:         A173C5A2C03DE08C025C93945B2E74B7
X[5]:         65D113682551614E556BFAA80AA2FA7A
GHASH(H,A,C): 2A807BDE4AF8A462D467D2FFA3E1D868
C:     13B4C72B389DC5018E72A171DD85A5D3
       752274D3A019FBCAED09A425CD9B2E1C
       9B72EEE7C9DE7D52B3F3
T:     D6A5284F4A6D3FE22A5D6C2B960494C3
```

C.5.2 GCM-AES-256 (54-octet frame confidentiality protection)

Table C-28 specifies an arbitrary 256-bit key (SAK), the Secure Data, and the ICV generated by the GCM-AES-256 Cipher Suite when that key is used in conjunction with the frame field data of Table C-25. The GCM parameter *P*, the data to be encrypted, is the User Data. The additional data *A* to be authenticated is formed by concatenating the MAC DA, the MAC SA, and the SecTAG. The SCI and the PN are concatenated (in that order) to form the 96-bit *IV* used by GCM. Details of the computation follow the table.

Table C-28—GCM-AES-256 Key, Secure Data, and ICV (example)

Field	Value
Key (SAK)	691D3EE909D7F54167FD1CA0B5D76908 1F2BDE1AEE655FDBAB80BD5295AE6BE7
Secure Data	C1 62 3F 55 73 0C 93 53 30 97 AD DA D2 56 64 96 61 25 35 2B 43 AD AC BD 61 C5 EF 3A C9 0B 5B EE 92 9C E4 63 0E A7 9F 6C E5 19
ICV	12 AF 39 C2 D1 FD C2 05 1F 8B 7B 3C 9D 39 7E F2

```
key size = 128 bits
P:     336 bits
A:     160 bits
IV:    96 bits
ICV:   128 bits
K:     691D3EE909D7F54167FD1CA0B5D76908
       1F2BDE1AEE655FDBAB80BD5295AE6BE7
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F30313233340004
A:     E20106D7CD0DF0761E8DCD3D88E54C2A
       76D457ED
IV:    F0761E8DCD3D000176D457ED
GCM-AES Encryption
H:            1E693C484AB894B26669BC12E6D5D776
Y[0]:         F0761E8DCD3D000176D457ED00000001
E(K,Y[0]):    87E183649AE3E7DBF725659152C39A22
Y[1]:         F0761E8DCD3D000176D457ED00000002
E(K,Y[1]):    C9623045621E80472581BAC2CB4C7F8A
C[1]:         C1623F55730C93533097ADDAD2566496
Y[2]:         F0761E8DCD3D000176D457ED00000003
E(K,Y[2]):    7C3B2A0B628F8F9944E3C812E02170C2
C[2]:         6125352B43ADACBD61C5EF3AC90B5BEE
Y[3]:         F0761E8DCD3D000176D457ED00000004
E(K,Y[3]):    BFB2CB533F95AC58E51D6608DBEBDBC2
C[3]:         929CE4630EA79F6CE519
X[1]:         F268EF5B38A96261A139D06CD7F43A33
X[2]:         9AE3BF42A20F4FB773EEFD5B5C5DBDD3
X[3]:         22A7FA0F7E5FC49715374D6B72EC7FBB
X[4]:         2FE103C6651C845A71217C1C7E80D559
X[5]:         FA94D93A0A7D235AEED7891F5E381A17
GHASH(H,A,C): 954EBAA64B1E25DEE8AE1EADCFFAE4D0
C:     C1623F55730C93533097ADDAD2566496
       6125352B43ADACBD61C5EF3AC90B5BEE
       929CE4630EA79F6CE519
T:     12AF39C2D1FDC2051F8B7B3C9D397EF2
```

C.5.3 GCM-AES-XPN-128 (54-octet frame confidentiality protection)

Table C-27 specifies arbitrary values for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), 96-bit Salt, and 128-bit key (SAK), with the Secure Data and ICV generated by the GCM-AES-XPN-128 Cipher Suite when used in conjunction with the foregoing and the frame field data of Table C-25. The GCM parameter P, the data to be encrypted, is the User Data. The additional data A to be authenticated is formed by concatenating the MAC DA, the MAC SA, and the SecTAG. The computed GCM parameter T is the ICV.

Table C-29—GCM-AES-XPN-128 Key, Secure Data, and ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	071B113B0CA743FECCCF3D051F737382
Secure Data	?? ??
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits
P:     336 bits
A:     160 bits
IV:    96 bits
ICV:   128 bits
K:     071B113B0CA743FECCCF3D051F737382
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F30313233340004
A:     E20106D7CD0DF0761E8DCD3D88E54C2A
       76D457ED
IV:    ????????????????????????
GCM-AES Encryption
H:            ????????????????????????????????
Y[0]:         ????????????????????????????????
E(K,Y[0]):    ????????????????????????????????
Y[1]:         ????????????????????????????????
E(K,Y[1]):    ????????????????????????????????
C[1]:         ????????????????????????????????
Y[2]:         ????????????????????????????????
E(K,Y[2]):    ????????????????????????????????
C[2]:         ????????????????????????????????
Y[3]:         ????????????????????????????????
E(K,Y[3]):    ????????????????????????????????
C[3]:         ????????????????????
X[1]:         ????????????????????????????????
X[2]:         ????????????????????????????????
X[3]:         ????????????????????????????????
X[4]:         ????????????????????????????????
X[5]:         ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:     ????????????????????????????????
       ????????????????????????????????
       ????????????????????
T:     ????????????????????????????????
```

C.5.4 GCM-AES-XPN-256 (54-octet frame confidentiality protection)

Table C-30 specifies arbitrary values for the 32 most significant bits of the 64-bit PN (the 32 least significant bits are those of the PN field in the SecTAG), a 96-bit Salt, and 256-bit key (SAK), with the Secure Data and ICV generated by the GCM-AES-XPN-256 Cipher Suite when used in conjunction with the foregoing and the frame field data of Table C-25. The GCM parameter P, the data to be encrypted, is the User Data. The additional data A to be authenticated is formed by concatenating the MAC DA, the MAC SA, and the SecTAG. The computed GCM parameter T is the ICV.

Table C-30—GCM-AES-XPN-256 Key, Secure Data, and ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	691D3EE909D7F54167FD1CA0B5D76908 1F2BDE1AEE655FDBAB80BD5295AE6BE7
Secure Data	?? ??
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits       P:     336 bits      A:     160 bits
IV:    96 bits            ICV:   128 bits
K:     691D3EE909D7F54167FD1CA0B5D76908
       1F2BDE1AEE655FDBAB80BD5295AE6BE7
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F30313233340004
A:     E20106D7CD0DF0761E8DCD3D88E54C2A
       76D457ED
IV:    ????????????????????????
GCM-AES Encryption
H:             ????????????????????????????????
Y[0]:          ????????????????????????????????
E(K,Y[0]):     ????????????????????????????????
Y[1]:          ????????????????????????????????
E(K,Y[1]):     ????????????????????????????????
C[1]:          ????????????????????????????????
Y[2]:          ????????????????????????????????
E(K,Y[2]):     ????????????????????????????????
C[2]:          ????????????????????????????????
Y[3]:          ????????????????????????????????
E(K,Y[3]):     ????????????????????????????????
C[3]:          ????????????????????
X[1]:          ????????????????????????????????
X[2]:          ????????????????????????????????
X[3]:          ????????????????????????????????
X[4]:          ????????????????????????????????
X[5]:          ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:     ????????????????????????????????
       ????????????????????????????????
       ????????????????????
T:     ????????????????????????????????
```

C.6 Confidentiality protection (60-octet frame)

Change the initial paragraphs and tables of clause C.6 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-31. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-31—Unprotected frame (example)

Field	Value
MAC DA	`D6 09 B1 F0 56 63`
MAC SA	`7A 0D 46 DF 99 8D`

User Data	`08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C`
	`1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C`
	`2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 00 02`

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, the PN, and the (optional) SCI. The fields of the protected frame are shown (in the order transmitted) in Table C-32.

Table C-32—Confidentiality protected frame (example)

Field	Value
MAC DA	`D6 09 B1 F0 56 63`
MAC SA	`7A 0D 46 DF 99 8D`
MACsec EtherType	`88 E5`
TCI and AN	`2E`
SL	`00`
PN	`B2 C2 84 65`
SCI	`12 15 35 24 C0 89 5E 81`
Secure Data	Cipher Suite and Key (SAK) dependent (see ~~Table C-23 and Table C-24~~ Table C-33, Table C-34, Table C-37, and Table C-38)
ICV	Cipher Suite and Key (SAK) dependent (see ~~Table C-23 and Table C-24~~ Table C-33, Table C-34, Table C-37, and Table C-38)

C.6.3 GCM-AES-XPN-128 (60-octet frame confidentiality protection)

Table C-35 specifies arbitrary values for the 32 most significant bits of the 64-bit PN, 96-bit Salt, and 128-bit key (SAK), with the Secure Data and ICV generated by the GCM-AES-XPN-128 Cipher Suite when used with the frame field data of Table C-31.

Table C-35—GCM-AES-XPN-128 Key, Secure Data, and ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	AD7A2BD03EAC835A6F620FDCB506B345
Secure Data	?? ??
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits
P:     384 bits
A:     224 bits
IV:    96 bits
ICV:   128 bits

K:     AD7A2BD03EAC835A6F620FDCB506B345

P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F303132333435363738393A0002

A:     D609B1F056637A0D46DF998D88E52E00
       B2C2846512153524C0895E81

IV:    ????????????????????????

GCM-AES Encryption
H:             ????????????????????????????????
Y[0]:          ????????????????????????????????
E(K,Y[0]):     ????????????????????????????????
Y[1]:          ????????????????????????????????
E(K,Y[1]):     ????????????????????????????????
C[1]:          ????????????????????????????????
Y[2]:          ????????????????????????????????
E(K,Y[2]):     ????????????????????????????????
C[2]:          ????????????????????????????????
Y[3]:          ????????????????????????????????
E(K,Y[3]):     ????????????????????????????????
C[3]:          ????????????????????????????????
X[1]:          ????????????????????????????????
X[2]:          ????????????????????????????????
X[3]:          ????????????????????????????????
X[4]:          ????????????????????????????????
X[5]:          ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????

C:     ????????????????????????????????
       ????????????????????????????????
       ????????????????????????????????

T:     ????????????????????????????????
```

C.6.4 GCM-AES-XPN-256 (60-octet frame confidentiality protection)

Table C-36 specifies arbitrary values for the 32 most significant bits of the 64-bit PN, 96-bit Salt, and 256-bit key (SAK), with the Secure Data and ICV generated by the GCM-AES-XPN-256 Cipher Suite when used with the frame field data of Table C-31.

Table C-36—GCM-AES-XPN-256 Key, Secure Data, and ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	E3C08A8F06C6E3AD95A70557B23F7548 3CE33021A9C72B7025666204C69C0B72
Secure Data	?? ??
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 256 bits
P:     384 bits
A:     224 bits
IV:    96 bits
ICV:   128 bits
K:     E3C08A8F06C6E3AD95A70557B23F7548
       3CE33021A9C72B7025666204C69C0B72
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F303132333435363738393A0002
A:     D609B1F056637A0D46DF998D88E52E00
       B2C2846512153524C0895E81
IV:    ????????????????????????
GCM-AES Encryption
H:            ????????????????????????????????
Y[0]:         ????????????????????????????????
E(K,Y[0]):    ????????????????????????????????
Y[1]:         ????????????????????????????????
E(K,Y[1]):    ????????????????????????????????
C[1]:         ????????????????????????????????
Y[2]:         ????????????????????????????????
E(K,Y[2]):    ????????????????????????????????
C[2]:         ????????????????????????????????
Y[3]:         ????????????????????????????????
E(K,Y[3]):    ????????????????????????????????
C[3]:         ????????????????????????????????
X[1]:         ????????????????????????????????
X[2]:         ????????????????????????????????
X[3]:         ????????????????????????????????
X[4]:         ????????????????????????????????
X[5]:         ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:     ????????????????????????????????
       ????????????????????????????????
       ????????????????????????????????
T:     ????????????????????????????????
```

C.7 Confidentiality protection (61-octet frame)

Change the initial paragraphs and tables of clause C.7 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-37. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-37—Unprotected frame (example)

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 00 06

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, the PN, and the (optional) SCI. The fields of the protected frame are shown (in the order transmitted) in Table C-38.

Table C-38—Confidentiality protected frame (example)

Field	Value
MAC DA	84 C5 D5 13 D2 AA
MAC SA	F6 E5 BB D2 72 77
MACsec EtherType	88 E5
TCI and AN	2F
SL	00
PN	89 32 D6 12
SCI	7C FD E9 F9 E3 37 24 C6
Secure Data	Cipher Suite and Key (SAK) dependent (see ~~Table -27 and Table C-28~~ Table C-39, Table C-40, Table C-41, and Table C-42)
ICV	Cipher Suite and Key (SAK) dependent (see ~~Table -27 and Table C-28~~ Table C-39, Table C-40, Table C-41, and Table C-42)

C.7.3 GCM-AES-XPN-128 (61-octet frame confidentiality protection)

Table C-41 specifies arbitrary values for the 32 most significant bits of the 64-bit PN, 96-bit Salt, and 128-bit key (SAK), with the Secure Data and ICV generated by the GCM-AES-XPN-128 Cipher Suite when used with the frame field data of Table C-37.

Table C-41—GCM-AES-XPN-128 Key, Secure Data, and ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	013FE00B5F11BE7F866D0CBBC55A7A90
Secure Data	?? ??
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits
P:     392 bits
A:     224 bits
IV:    96 bits
ICV:   128 bits
K:     013FE00B5F11BE7F866D0CBBC55A7A90
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F303132333435363738393A3B00
       06
A:     84C5D513D2AAF6E5BBD2727788E52F00
       8932D6127CFDE9F9E33724C6
IV:    ????????????????????????
GCM-AES Encryption
H:            ????????????????????????????????
Y[0]:         ????????????????????????????????
E(K,Y[0]):    ????????????????????????????????
Y[1]:         ????????????????????????????????
E(K,Y[1]):    ????????????????????????????????
C[1]:         ????????????????????????????????
Y[2]:         ????????????????????????????????
E(K,Y[2]):    ????????????????????????????????
C[2]:         ????????????????????????????????
Y[3]:         ????????????????????????????????
E(K,Y[3]):    ????????????????????????????????
C[3]:         ????????????????????????????????
Y[4]:         ????????????????????????????????
E(K,Y[4]):    ????????????????????????????????
C[4]:         ??
X[1]:         ????????????????????????????????
X[2]:         ????????????????????????????????
X[3]:         ????????????????????????????????
X[4]:         ????????????????????????????????
X[5]:         ????????????????????????????????
X[6]:         ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:     ????????????????????????????????
       ????????????????????????????????
       ????????????????????????????????
       ??
T:     ????????????????????????????????
```

C.7.4 GCM-AES-XPN-256 (61-octet frame confidentiality protection)

Table C-42 specifies arbitrary values for the 32 most significant bits of the 64-bit PN, 96-bit Salt, and 256-bit key (SAK), with the Secure Data and ICV generated by the GCM-AES-XPN-256 Cipher Suite when used with the frame field data of Table C-37.

Table C-42—GCM-AES-XPN-256 Key, Secure Data, and ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	83C093B58DE7FFE1C0DA926AC43FB360 9AC1C80FEE1B624497EF942E2F79A823
Secure Data	?? ??
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 256 bits        P:     392 bits      A:     224 bits
IV:    96 bits             ICV:   128 bits
K:     83C093B58DE7FFE1C0DA926AC43FB360
       9AC1C80FEE1B624497EF942E2F79A823
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F303132333435363738393A3B00
       06
A:     84C5D513D2AAF6E5BBD2727788E52F00
       8932D6127CFDE9F9E33724C6
IV:    ????????????????????????
GCM-AES Encryption
H:             ????????????????????????????????
Y[0]:          ????????????????????????????????
E(K,Y[0]):     ????????????????????????????????
Y[1]:          ????????????????????????????????
E(K,Y[1]):     ????????????????????????????????
C[1]:          ????????????????????????????????
Y[2]:          ????????????????????????????????
E(K,Y[2]):     ????????????????????????????????
C[2]:          ????????????????????????????????
Y[3]:          ????????????????????????????????
E(K,Y[3]):     ????????????????????????????????
C[3]:          ????????????????????????????????
Y[4]:          ????????????????????????????????
E(K,Y[4]):     ????????????????????????????????
C[4]:          ??
X[1]:          ????????????????????????????????
X[2]:          ????????????????????????????????
X[3]:          ????????????????????????????????
X[4]:          ????????????????????????????????
X[5]:          ????????????????????????????????
X[6]:          ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:     ????????????????????????????????
       ????????????????????????????????
       ????????????????????????????????
       ??
T:     ????????????????????????????????
```

C.8 Confidentiality protection (75-octet frame)

Change the initial paragraphs and tables of clause C.8 as follows:

The MAC Destination Address, MAC Source Address, and MAC Service Data Unit (MSDU, User Data) of a MAC Service data request and a corresponding data indication are shown in Table C-43. These comprise the octets of an unprotected frame when concatenated in the order given (with the addition of any media dependent additional fields such as padding). The User Data shown includes the IP EtherType.

Table C-43—Unprotected frame (example)

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
User Data	08 00 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30 31 32 33 34 35 36 37 38 39 3A 3B 3C 3D 3E 3F 40 41 42 43 44 45 46 47 48 49 00 08

The MAC Security TAG comprises the MACsec EtherType, the TCI, the AN, the SL, and the PN. The optional SCI has been omitted. The fields of the protected frame are shown (in the order transmitted) in Table C-44.

Table C-44—Confidentiality protected frame (example)

Field	Value
MAC DA	68 F2 E7 76 96 CE
MAC SA	7A E8 E2 CA 4E C5
MACsec EtherType	88 E5
TCI and AN	4D
SL	00
PN	2E 58 49 5C
Secure Data	Cipher Suite and Key (SAK) dependent (see ~~Table C-31 and Table C-32~~ Table C-45, Table C-46, Table C-47, and Table C-48)
ICV	Cipher Suite and Key (SAK) dependent (see ~~Table C-31 and Table C-32~~ Table C-45, Table C-46, Table C-47, and Table C-48)

C.8.3 GCM-AES-XPN-128 (75-octet frame confidentiality protection)

Table C-47 specifies arbitrary values for the 32 most significant bits of the 64-bit PN, 96-bit Salt, and 128-bit key (SAK), with the Secure Data and ICV generated by the GCM-AES-XPN-128 Cipher Suite when used with the frame field data of Table C-43.

Table C-47—GCM-AES-XPN-128 Key, Secure Data, and ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	88EE087FD95DA9FBF6725AA9D757B0CD
Secure Data	?? ??
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 128 bits
P:     504 bits
A:     160 bits
IV:    96 bits
ICV:   128 bits
K:     88EE087FD95DA9FBF6725AA9D757B0CD
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F303132333435363738393A3B3C
       3D3E3F404142434445464748490008
A:     68F2E77696CE7AE8E2CA4EC588E54D00
       2E58495C
IV:    ????????????????????????
GCM-AES Encryption
H:             ????????????????????????????????
Y[0]:          ????????????????????????????????
E(K,Y[0]):     ????????????????????????????????
Y[1]:          ????????????????????????????????
E(K,Y[1]):     ????????????????????????????????
C[1]:          ????????????????????????????????
Y[2]:          ????????????????????????????????
E(K,Y[2]):     ????????????????????????????????
C[2]:          ????????????????????????????????
Y[3]:          ????????????????????????????????
E(K,Y[3]):     ????????????????????????????????
C[3]:          ????????????????????????????????
Y[4]:          ????????????????????????????????
E(K,Y[4]):     ????????????????????????????????
C[4]:          ??????????????????????????????
X[1]:          ????????????????????????????????
X[2]:          ????????????????????????????????
X[3]:          ????????????????????????????????
X[4]:          ????????????????????????????????
X[5]:          ????????????????????????????????
X[6]:          ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:     ????????????????????????????????
       ????????????????????????????????
       ????????????????????????????????
       ??????????????????????????????
T:     ????????????????????????????????
```

C.8.4 GCM-AES-XPN-256 (75-octet frame confidentiality protection)

Table C-48 specifies arbitrary values for the 32 most significant bits of the 64-bit PN, 96-bit Salt, and 256-bit key (SAK), with the Secure Data and ICV generated by the GCM-AES-XPN-256 Cipher Suite when used with the frame field data of Table C-43.

Table C-48—GCM-AES-XPN-256 Key, Secure Data, and ICV (example)

Field	Value
PN (ms 32-bits)	B0DF459C
Salt	E630E81A48DF
Key (SAK)	4C973DBC7364621674F8B5B89E5C1551 1FCED9216490FB1C1A2CAA0FFE0407E5
Secure Data	?? ??
ICV	?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??

```
key size = 256 bits        P:     504 bits      A:     160 bits
IV:    96 bits             ICV:   128 bits
K:     4C973DBC7364621674F8B5B89E5C1551
       1FCED9216490FB1C1A2CAA0FFE0407E5
P:     08000F101112131415161718191A1B1C
       1D1E1F202122232425262728292A2B2C
       2D2E2F303132333435363738393A3B3C
       3D3E3F404142434445464748490008
A:     68F2E77696CE7AE8E2CA4EC588E54D00
       2E58495C
IV:    ????????????????????????
GCM-AES Encryption
H:             ????????????????????????????????
Y[0]:          ????????????????????????????????
E(K,Y[0]):     ????????????????????????????????
Y[1]:          ????????????????????????????????
E(K,Y[1]):     ????????????????????????????????
C[1]:          ????????????????????????????????
Y[2]:          ????????????????????????????????
E(K,Y[2]):     ????????????????????????????????
C[2]:          ????????????????????????????????
Y[3]:          ????????????????????????????????
E(K,Y[3]):     ????????????????????????????????
C[3]:          ????????????????????????????????
Y[4]:          ????????????????????????????????
E(K,Y[4]):     ????????????????????????????????
C[4]:          ??????????????????????????????
X[1]:          ????????????????????????????????
X[2]:          ????????????????????????????????
X[3]:          ????????????????????????????????
X[4]:          ????????????????????????????????
X[5]:          ????????????????????????????????
X[6]:          ????????????????????????????????
GHASH(H,A,C): ????????????????????????????????
C:     ????????????????????????????????
       ????????????????????????????????
       ????????????????????????????????
       ??????????????????????????????
T:     ????????????????????????????????
```