IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 1: Galois Counter Mode— Advanced Encryption Standard— 256 (GCM-AES-256) Cipher Suite

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

14 October 2011

IEEE Std 802.1AEbn™-2011
(Amendment to
IEEE Std 802.1AE™-2006)

IEEE Std 802.1AEbn™-2011
(Amendment to
IEEE Std 802.1AE™-2006)

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 1: Galois Counter Mode—Advanced Encryption Standard—256 (GCM-AES-256) Cipher Suite

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 10 September 2011

IEEE-SA Standards Board

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: authenticity, authorized port, confidentiality, data origin integrity, IEEE 802.1AEbn, 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 978-0-7381-6735-0 STD97152
Print: ISBN 978-0-7381-6736-7 STDPD97152

Introduction

This introduction is not part of IEEE Std 802.1AEbn-2011, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Security—Amendment 1: Galois Counter Mode—Advanced Encryption Standard—256 (GCM-AES-256) Cipher Suite.

The first edition of IEEE Std 802.1AE was published in 2006. This first amendment to that standard adds the option of using the GCM-AES-256 Cipher Suite.

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. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association website at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/findstds/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/findstds/interps/index.html.

Patents

Attention is called to the possibility that implementation of this amendment may require use of subject matter covered by patent rights. By publication of this amendment, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this amendment are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA for approval, the IEEE P802.1 Working Group had the following membership:

Tony Jeffree, *Chair*
Paul Congdon, *Vice Chair*
Mick Seaman, *Editor* and *Chair, Security Task Group*

Zehavit Alon
Yafan An
Ting Ao
Peter Ashwood-Smith
Christian Boiger
Paul Bottorff
Rudolf Brandner
Craig Carlson
Rodney Cummings
Claudio Desanti
Zhemin Ding
Donald Eastlake, III
Janos Farkas
Donald Fedyk
Norman Finn
Ilango Ganga
Geoffrey Garner
Anoop Ghanwani
Mark Gravel
Eric Gray
Yingjie Gu
Craig Gunther
Michael Johas Teener
Stephen Haddock
Hitoshi Hayakawa
Hal Keen
Srikanth Keesara
Yongbum Kim
Philippe Klein
Oliver Kleineberg
Michael Krause
Lin Li
Jeff Lynch
Ben Mack-Crane
David Martin
John Messenger
John Morris
Eric Multanen
David Olsen
Donald Pannell
Glenn Parsons
Mark Pearson
Joseph Pelissier
Rene Raeber
Karen T. Randall
Josef Roese
Dan Romascanu
Jessy Rouyer
Ali Sajassi
Panagiotis Saltsidis
Rakesh Sharma
Kevin Stanton
Robert Sultan
PatriciaThaler
Chait Tumuluri
Maarten Vissers

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

Thomas Alexander
Butch Anton
Nancy Bravin
William Byrd
Radhakrishna Canchi
Keith Chow
Charles Cook
Claudio DeSanti
Wael Diab
Patrick Diamond
Thomas Dineen
Sourav Dutta
Donald Fedyk
Yukihiro Fujimoto
Devon Gayle
Gregory Gillooly
Evan Gilman
Ron Greenthaler
Randall Groves
C. Guy
John Hawkins
David Hunter
Paul Isaacs
Atsushi Ito
Raj Jain
Junghoon Jee
Tony Jeffree
Michael Johas Teener
Shinkyo Kaku
Piotr Karocki
Stuart J. Kerry
Lior Khermosh
Yongbum Kim
Geoff Ladwig
Paul Lambert
William Lumpkins
Greg Luri
Elvis Maculuba
Edward McCall
Michael McInnis
Gary Michel
Michael S. Newman
Satoshi Obara
Glenn Parsons
Karen T. Randall
Maximilian Riegel
Robert Robinson
Benjamin Rolfe
Jessy Rouyer
Herbert Ruck
Randall Safier
Joseph Salowey
Raymond Savarda
Bartien Sayogo
Mick Seaman
Shusaku Shimada
Kapil Sood
Thomas Starai
Walter Struppler
Joseph Tardo
Michael Johas Teener
Patricia Thaler
Mark-Rene Uchida
Dmitri Varsanofiev
Prabodh Varshney
John Vergis
Hung-Yu Wei
Brian Weis
Ludwig Winkel
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 10 September 2011, it had the following membership:

Contents

1. Overview 2

1.1 Introduction 2
1.2 Scope 2

2. Normative references 3

6. Secure provision of the MAC Service 4

6.1 MACsec connectivity 4

7. Principles of secure network operation 5

8. MAC Security Protocol (MACsec) 6

9. Encoding of MACsec protocol data units 7

9.8 Transmit SA status 7

10. Principle of MAC Security Entity (SecY) operation 8

11. MAC Security in Systems 9

11.7 MACsec in Provider Bridged Networks 9

14. Cipher Suites 10

14.1 Cipher Suite use 10
14.4 Cipher Suite conformance 10
14.5 Default Cipher Suite (GCM-AES-128) 11
14.6 GCM-AES-256 11

Annex B (informative) Bibliography 13

Annex C (informative) MACsec Test Vectors 14

C.1 Integrity protection (54-octet frame) 15
C.2 Integrity protection (60-octet frame) 18
C.3 Integrity protection (65-octet frame) 21
C.4 Integrity protection (79-octet frame) 24
C.5 Confidentiality protection (54-octet frame) 27
C.6 Confidentiality protection (60-octet frame) 30
C.7 Confidentiality protection (61-octet frame) 33
C.8 Confidentiality protection (75-octet frame) 36

Figures

Figure 11-14 Provider network with priority selection and aggregation 9
Figure 14-1 Cipher Suite Protect and Validate operations 10

Tables

Table 14-1 MACsec Cipher Suites 10
Table C-1 Unprotected frame (example) 15
Table C-2 Integrity protected frame (example) 15
Table C-3 GCM-AES-128 Key and calculated ICV (example) 16
Table C-4 GCM-AES-256 Key and calculated ICV (example) 17
Table C-5 Unprotected frame (example) 18
Table C-6 Integrity protected frame (example) 18
Table C-7 GCM-AES-128 Key and calculated ICV (example) 19
Table C-8 GCM-AES-256 Key and calculated ICV (example) 20
Table C-9 Unprotected frame (example) 21
Table C-10 Integrity protected frame (example) 21
Table C-11 GCM-AES-128 Key and calculated ICV (example) 22
Table C-12 GCM-AES-256 Key and calculated ICV (example) 23
Table C-13 Unprotected frame (example) 24
Table C-14 Integrity protected frame (example) 24
Table C-15 GCM-AES-128 Key and calculated ICV (example) 25
Table C-16 GCM-AES-256 Key and calculated ICV (example) 26
Table C-17 Unprotected frame (example) 27
Table C-18 Confidentiality protected frame (example) 27
Table C-19 GCM-AES-128 Key, Secure Data, and ICV (example) 28
Table C-20 GCM-AES-256 Key, Secure Data, and ICV (example) 29
Table C-21 Unprotected frame (example) 30
Table C-22 Confidentiality protected frame (example) 30
Table C-23 GCM-AES-128 Key, Secure Data, and ICV (example) 31
Table C-24 GCM-AES-256 Key, Secure Data, and ICV (example) 32
Table C-25 Unprotected frame (example) 33
Table C-26 Confidentiality protected frame (example) 33
Table C-27 GCM-AES-128 Key, Secure Data, and ICV (example) 34
Table C-28 GCM-AES-256 Key, Secure Data, and ICV (example) 35
Table C-29 Unprotected frame (example) 36
Table C-30 Confidentiality protected frame (example) 36
Table C-31 GCM-AES-128 Key, Secure Data, and ICV (example) 37
Table C-32 GCM-AES-256 Key, Secure Data, and ICV (example) 38

IEEE Standard for
Local and metropolitan area networks—

Media Access Control (MAC) Security

Amendment 1: Galois Counter Mode—Advanced Encryption Standard—256 (GCM-AES-256) Cipher Suite

IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at http://standards.ieee.org/IPR/disclaimers.html.

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

1.1 Introduction

Change the fourth paragraph as follows:

To deliver these benefits, MACsec has to be used in conjunction with appropriate policies for higher-level protocol operation in networked systems, an authentication and authorization framework, and network management. IEEE Std 802.1X ~~P802.1af™ [B2]~~[1] provides authentication and cryptographic key distribution.

1.2 Scope

Change bullet i) as follows:

i) Specifies the interface/exchanges between a SecY and its associated and collocated MAC Security Key Agreement Entity (KaY, IEEE Std 802.1X ~~P802.1af [B2]~~) that provides and updates cryptographic keys.

Change bullet o) as follows:

o) Specify how the relationships between MACsec protocol peers are discovered and authenticated, as supported by key management or key distribution protocols, but makes use of IEEE Std 802.1X ~~P802.1af Key Agreement for MAC security~~ to achieve these functions.

2. Normative references

Insert the following references at the appropriate point:

IEEE Std 802.1X™-2010, IEEE Standard for Local and Metropolitan Area Networks: Port-based Network Access Control.

IEEE Std 802.1Q™, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

NIST SP 800-38D, Nov 2007, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.[1]

Delete the following reference and the accompanying footnote:

~~Galois Counter Mode of Operation (GCM), David A. McGrew, John Viega.~~[4]

Delete the following references:

~~IEEE Std 802.1Q-2005, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.~~

~~IEEE Std 802.1X-2004, IEEE Standard for Local and Metropolitan Area Networks: Port Based Network Access Control.~~

~~IEEE Std 802.1ad™-2005, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.~~

[1]This document is available at http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

6. Secure provision of the MAC Service

6.1 MACsec connectivity

Change the first paragraph as follows:

The connectivity provided (6.2) between the MAC Internal Sublayer Service (ISS) access points of stations connected to a single LAN composes an insecure association between communicating stations. Key agreement protocols as defined in ~~IEEE P802.1af~~ IEEE Std 802.1X establish and maintain a secure Connectivity Association (CA), which is a fully (i.e., symmetric and transitive) connected subset of the ISS service access points. Each instance of MACsec operates within a single CA.

7. Principles of secure network operation

Change bullet d) as follows:

d) MACsec Key Agreement Entities (~~IEEE P802.1af~~IEEE Std 802.1X)

7.1.2 Use of the secure MAC Service by bridges

Change NOTE 1 as follows:

NOTE 1—Using an SC identifier that includes a port number component would appear to be unnecessary in the case of a simple system that comprises a single LAN station, with a uniquely allocated 48-bit MAC address, and a single SecY. However, some systems require support for more SecYs than they have uniquely allocated addresses, either because they make use of technologies that support virtual MACs, or because their interface stacks include the possibility of including multiple SecYs at different sublayers. Provider bridges (~~IEEE Std 802.1ad-2005~~IEEE Std 802.1Q) provide examples of the latter.

7.3.1 Client policies

Change NOTE 1 as follows:

NOTE 1—To facilitate policy selection by clients of the secure MAC Service, ~~IEEE P802.1af~~ IEEE Std 802.1X specifies authorized permissions, including those required by MAC Bridges (IEEE Std 802.1D) and VLAN-aware Bridges (IEEE Std 802.1Q) to support the secure MAC Service in Bridged and Virtually Bridged Local Area Networks.

7.3.2 Use of the secure MAC Service by bridges

Change NOTE 1 as follows:

NOTE 1—The apparent exception to this configuration restriction, which does not permit the creation of security associations to create "secure tunnels" through selected bridges in a Bridged Local Area Network, is the use of a Provider Bridged Network as specified in ~~IEEE Std 802.1ad-2005~~IEEE Std 802.1Q. However, a Provider Bridged Network appears to Customer Bridges as a single LAN providing full connectivity independent of the operation of Customer Bridge protocols.

Change NOTE 2 as follows:

NOTE 2—Use of this address ensures that the physical topology as perceived by spanning tree protocols aligns with that provided by MAC Security. In Provider Bridged Networks, the Provider Bridge Group Address is used. An exception to the alignment rule occurs with certain types of interface that are supported by Provider Bridge Networks, where a provider operated C-VLAN (see ~~IEEE Std 802.1ad-2005~~IEEE Std 802.1Q) aware component provides the customer interface.

Change bullet d) as follows:

d) Configuration of the VLAN Translation Table ~~(IEEE Std 802.1ad-2005 only)~~

Change NOTE 3 as follows:

NOTE 3—A Bridge Port is one of the bridge's points of attachment to an instance of the MAC Internal Sublayer Service (ISS), and is used by the MAC Relay Entity and associated Higher-Layer Entities as specified in IEEE Std 802.1D~~,~~ and IEEE Std 802.1Q~~, and IEEE Std 802.1ad~~.

8. MAC Security Protocol (MACsec)

8.1.3 Interoperability requirements

Change the third paragraph as follows:

Where the underlying MAC Service used by MACsec is supported by a Provider Bridged Network (~~IEEE Std 802.1ad~~IEEE Std 802.1Q), communicating SecYs can be attached to different media operating (locally) at different transmission rates. Interoperability between, for example, 10 Gb/s and 1 Gb/s, and between 1 Gb/s and 100 Mb/s requires interoperability across the speed range. The design of MACsec facilitates interoperability from 1 Mb/s to 100 Gb/s without modification or negotiation of protocol formats and parameters. Operation at higher transmission rates depends on the capabilities of the Cipher Suite. The mandatory default Cipher Suite has been selected (Clause 14) in part because of its ability to perform across this range.

9. Encoding of MACsec protocol data units

9.8 Transmit SA status

Change the NOTE, as follows:

NOTE~~— As specified in this clause, the~~ The IV used by the ~~d~~Default Cipher Suite ~~(~~GCM-AES-128~~)~~ (14.5) and the GCM-AES-256 Cipher Suite (14.6) comprises the SCI (even if the SCI is not transmitted in the SecTAG) and the 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.

10. Principle of MAC Security Entity (SecY) operation

10.7.22 Transmit SA status

Insert a further bullet e) directly after the existing bullet d), as follows:

e) nextPN (10.6, 10.6.5)

11. MAC Security in Systems

11.7 MACsec in Provider Bridged Networks

Change the first paragraph as follows:

~~Provider Bridges are specified in the IEEE Std 802.1ad amendment to IEEE Std 802.1Q.~~ Provider Bridges (IEEE Std 802.1Q) enable service providers to use VLANs to offer the equivalent of separate LANs to different users. Data for each of the virtual LANs is segregated within the provider's network by using a Service VLAN TAG (S-TAG) that is distinguished, by EtherType, from the Customer VLAN-TAGs (C-TAGs) used within each customer's network. See Figure 11-12.

Change the NOTE as follows:

NOTE—Figure 11-12 is based on Figure 15-1 of ~~IEEE Std 802.1ad-2005~~IEEE Std 802.1Q.

Change the paragraph describing Figure 11-14 as follows:

Figure 11-14 shows the addition of the service access priority selection function described in 6.9 of ~~IEEE Std 802.1ad~~IEEE Std 802.1Q to the interface stack of Figure 11-13, together with the use of Link Aggregation to support attachment to the provider's network with two LANs.

Replace Figure 11-14 with the following figure, which changes the prior reference to IEEE Std 802.1ad Clause 6.9 to a reference to IEEE Std 802.1Q Clause 6.9:

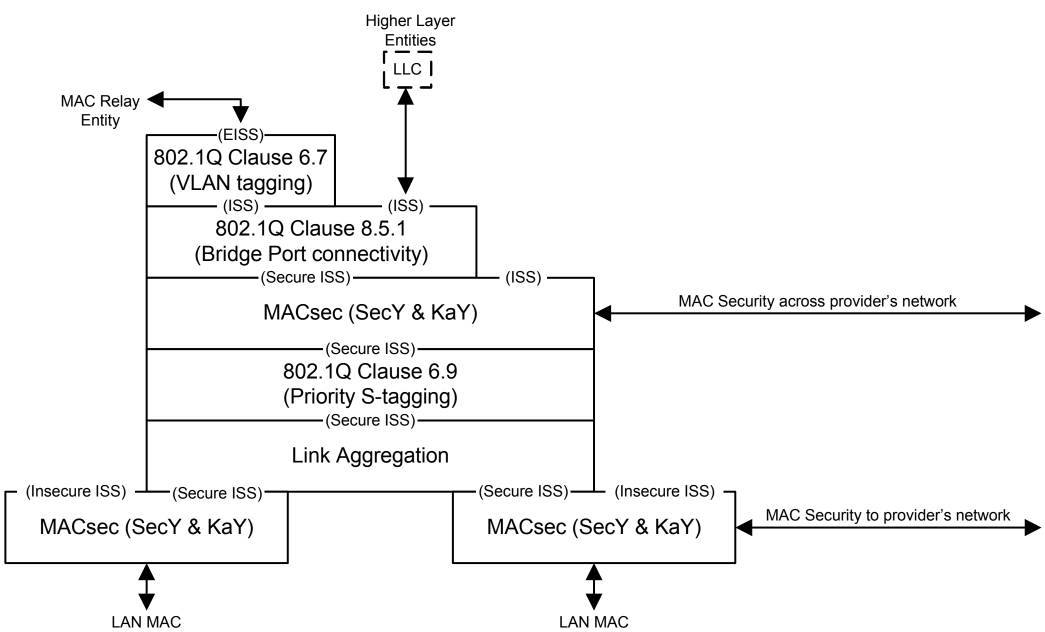
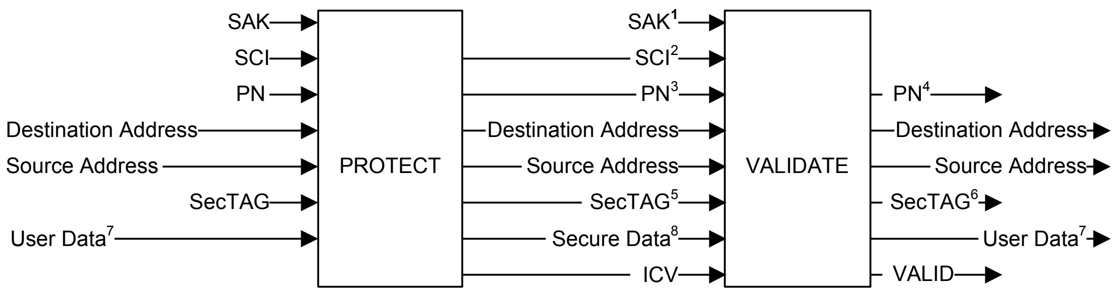


Figure 11-14—Provider network with priority selection and aggregation

14. Cipher Suites

14.1 Cipher Suite use

Change footnote 2 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.

[3] The PN 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

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		
~~00-80-02-00-01-00-00-01~~ 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

Delete the NOTE after the table as follows:

~~NOTE—Currently, Table 14-1 does not include any optional Cipher Suites.~~

Insert the following NOTE after the paragraph beginning "Table 14-1 assigns a Cipher Suite reference number for use in protocol identification within a MACsec context":

NOTE—In IEEE Std 802.1AE-2006 (the first edition of this standard) the Cipher Suite Identifier for GCM-AES-128 was incorrectly shown as 00-80-02-00-01-00-00-01 in Table 14-1. Prior to the inclusion of GCM-AES-256, GCM-AES-128 was the only conformant Cipher Suite. IEEE Std 802.1X uses a reserved encoding for the Default Cipher Suite rather than the Cipher Suite Identifier to identify GCM-AES-128.

Change 14.5 as follows:

14.5 Default Cipher Suite (GCM-AES-128)

The Default Cipher Suite uses the Galois/Counter Mode of ~~O~~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 ~~section 2.1 of the GCM specification (GCM) as submitted to NIST~~ NIST SP 800-38D.

K is the 128 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 toIEEE 802.3 "wire order" for frame transmission.

When the Default 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 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 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 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 toIEEE 802.3 "wire order" for frame transmission.

When the Default 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 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 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.

Annex B

(informative)

Bibliography

Delete bibiographical reference [B2] and the accompanying footnote as follows, renumbering other bibliographical references and updating cross-references as necessary.

~~[B2] IEEE P802.1af, Draft Standard for Key Agreement for MAC Security.[3]~~

Insert the following bibliographical references in alphanumerical order, renumbering other bibliographical references and updating cross-references as necessary:

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

[Bxx] The Galois/Counter Mode of Operation (GCM), David A. McGrew and J. Viega. May 31, 2005.[4]

[Bxx] The Security and Performance of the Galois/Counter Mode (GCM) of Operation. D. McGrew and J. Viega. Proceedings of INDOCRYPT '04, Springer-Verlag, 2004.[5]

~~[3]Numbers preceded by P are IEEE authorized standards projects that were not approved by the IEEE-SA Standards Board at the time this publication went to press. (The most recent draft should be used.) For information about obtaining drafts, contact the IEEE.~~

[4]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

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

Insert new Annex C, as follows:

Annex C

(informative)

MACsec Test Vectors

This annex provides test case examples of the use of MACsec. Each example shows an unprotected frame that could be transmitted as a result of a MAC Service request (with a given set of parameters) and the corresponding MACsec protected frame (with a given set of MACsec SecY parameters). Test cases include the use of integrity protection without confidentiality (authenticated, but unencrypted) and the use of both integrity protection and confidentiality (authenticated and encrypted).

The test cases use a number of different unprotected frame sizes. Two correspond to common sizes of internet packets, 54 octets and 60 octets—two common representations of a TCP/IP SYN packet. A TCP SYN comprises 40 octets plus 14 octets of MAC DA+SA+Ethertype. The frame could be padded to 60 octets to meet minimum Ethernet frame length requirements prior to MACsec processing. The remaining frame sizes represent “corner cases” of the GCM padding algorithm. A 61-octet frame, when encrypted, has a 49-octet payload, which results in the maximum 15 octets of padding for ICV calculation. When integrity protection is provided but confidentiality is not (i.e., when the user data is not encrypted) a 65-octet frame also requires that maximum padding. A 75-octet frame has a 63 octet payload, requiring 1 octet of padding for ICV calculation, as does a 79-octet frame that is integrity protected without confidentiality. The zero-octet padding case is covered by the 60-octet frame, above. MACsec processing is performed above the media-dependent functions of media access control, so all frame sizes given are prior to the addition of the 32-bit CRC or other media dependent fields.

Test cases are provided for both the Default Cipher Suite (GCM-AES-128, 14.5) and GCM-AES-256 (14.6). 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)

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, 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)

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)

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. 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)

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. 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
```

C.2 Integrity protection (60-octet frame)

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-5. 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-5—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-6.

Table C-6—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)

C.2.1 GCM-AES-128 (60-octet frame integrity protection)

Table C-7 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-5. Details of the computation follow the table.

Table C-7—GCM-AES-128 Key and calculated ICV (example)

Field	Value
Key (SAK)	071B113B0CA743FECCCF3D051F737382
ICV	0C 01 7B C7 3B 22 7D FC C9 BA FA 1C 41 AC C3 53

```
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:    F0761E8DCD3D000176D457ED
GCM-AES Authentication
H:     E4E01725D724C1215C7309AD34539257
Y[0]:  F0761E8DCD3D000176D457ED00000001
E(K,Y[0]): FC25539100959B80FE3ABED435E54CAB
X[1]:  8DAD4981E33493018BB8482F69E4478C
X[2]:  5B0BFA3E67A3E080CB60EA3D523C734A
X[3]:  051F8D267A68CF88748E56C5F64EF503
X[4]:  4187F1240DB1887F2A92DDAB8903A0F6
X[5]:  C7D64941A90F02FA9FCDECC083B4B276
GHASH(H,A,C): F02428563BB7E67C378044C874498FF8
C:
T:     0C017BC73B227DFCC9BAFA1C41ACC353
```


C.2.2 GCM-AES-256 (60-octet frame integrity protection)

Table C-8 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-6. Details of the computation follow the table.

Table C-8—GCM-AES-256 Key and calculated ICV (example)

Field	Value
Key (SAK)	691D3EE909D7F54167FD1CA0B5D76908 1F2BDE1AEE655FDBAB80BD5295AE6BE7
ICV	35 21 7C 77 4B BC 31 B6 31 66 BC F9 D4 AB ED 07

```
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:    F0761E8DCD3D000176D457ED
GCM-AES Authentication
H:     1E693C484AB894B26669BC12E6D5D776
Y[0]:  F0761E8DCD3D000176D457ED00000001
E(K,Y[0]): 87E183649AE3E7DBF725659152C39A22
X[1]:  20107B262134C35B60499E905C532004
X[2]:  D7A468F455F09F947884E35A2C80CD7F
X[3]:  A82D607070F2E4470FD94C0EECA9FCC1
X[4]: 03C3C8725883EB355963BD53B515C82D
X[5]: 8FF6F0311DDE274FFA936965C0C905B4
GHASH(H,A,C): B2C0FF13D15FD66DC643D96886687725
C:
T: 35217C774BBC31B63166BCF9D4ABED07
```

C.3 Integrity protection (65-octet frame)

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-9. 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-9—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-10.

Table C-10—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	Cipher Suite and Key (SAK) dependent (see Table C-11 and Table C-12)

C.3.1 GCM-AES-128 (65-octet frame integrity protection)

Table C-11 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-10. Details of the computation follow the table.

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

Field	Value
Key (SAK)	013FE00B5F11BE7F866D0CBBC55A7A90
ICV	21 78 67 E5 0C 2D AD 74 C2 8C 3B 50 AB DF 69 5A

```
key size = 128 bits
P:      0 bits
A:      648 bits
IV:     96 bits
ICV:    128 bits
K:      013FE00B5F11BE7F866D0CBBC55A7A90
P:
A:      84C5D513D2AAF6E5BBD2727788E52300
        8932D6127CFDE9F9E33724C608000F10
        1112131415161718191A1B1C1D1E1F20
        2122232425262728292A2B2C2D2E2F30
        313233343536373839 3A3B3C3D3E3F00
        05
IV:     7CFDE9F9E33724C68932D612
GCM-AES Authentication
H:      EB28DCB361EE1110F98CA0C9A07C88F7
Y[0]:  7CFDE9F9E33724C68932D61200000001
E(K,Y[0]): 4EAAF8E4DF948ACAC7F3349C1006A91F
X[1]:  279344E391DB8834EFA68FD3F1BA5CD8
X[2]:  DC35B123F4D387BBB076D0822BD60816
X[3]:  8AB3B52963CC15C9C2DB3E4C801CB65A
X[4]:  CAB6A261225F42578E6B86ABA9F0DD18
X[5]:  6ABDBB3ECAC0458F116A82AA0DAC563F
X[6]:  8F39EF45985C691E35814202B6BB6EF6
GHASH(H,A,C): 6FD29F01D3B927BE057F0FCCBBD9C045
C:
T:      217867E50C2DAD74C28C3B50ABDF695A
```

C.3.2 GCM-AES-256 (65-octet frame integrity protection)

Table C-12 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-10. Details of the computation follow the table.

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

Field	Value
Key (SAK)	83C093B58DE7FFE1C0DA926AC43FB360 9AC1C80FEE1B624497EF942E2F79A823
ICV	6E E1 60 E8 FA EC A4 B3 6C 86 B2 34 92 0C A9 75

```
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:    7CFDE9F9E33724C68932D612
GCM-AES Authentication
H:     D03D3B51FDF2AACB3A165D7DC362D929
Y[0]:  7CFDE9F9E33724C68932D61200000001
E(K,Y[0]): E97EA8EE4455AE79EC4225CAC340E326
X[1]:  22C28F4DF8D09267EA3E11F019F5932C
X[2]:  3D02CFE5FC6A8A9E65B8FFD63E525083
X[3]:  78466AE4A3490819A08645DDC95B143B
X[4]: 6FE4921A6F0A1D5DD90A100A40206142
X[5]: C880DEC2FF2C44F8AD611692AF6D1069
X[6]:  CF4D709A4D020BA876F4371BAA788444
GHASH(H,A,C): 879FC806BEB90ACA80C497FE514C4A53
C:
T: 6EE160E8FAECA4B36C86B234920CA975
```

C.4 Integrity protection (79-octet frame)

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	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-14.

Table C-14—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	Cipher Suite and Key (SAK) dependent (see Table C-15 and Table C-16)

C.4.1 GCM-AES-128 (79-octet frame integrity protection)

Table C-11 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-14. Details of the computation follow the table.

Table C-15—GCM-AES-128 Key and calculated ICV (example)

Field	Value
Key (SAK)	88EE087FD95DA9FBF6725AA9D757B0CD
ICV	07 92 2B 8E BC F1 0B B2 29 75 88 CA 4C 61 45 23

```
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:    7AE8E2CA4EC500012E58495C
GCM-AES Authentication
H:     AE19118C3B704FCE42AE0D15D2C15C7A
Y[0]:  7AE8E2CA4EC500012E58495C00000001
E(K,Y[0]): D2521AABC48C06033E112424D4A6DF74
X[1]:  CA0CAE2BEE8F19845DCB7FE3C5E713AB
X[2]:  5D3F9C7A3BC869457EA5FDFD404A415F
X[3]:  760E6A2873ACC0515D4901B5AC1C85E4
X[4]:  5A40A8425165E3D1978484F07AFC70D8
X[5]:  D9687630FC4436EE582A90A8E4AFC504
X[6]:  311CE361065F86403CDA5DB00798B961
GHASH(H,A,C): D5C03125787D0DB11764ACEE98C79A57
C:
T:     07922B8EBCF10BB2297588CA4C614523
```

C.4.2 GCM-AES-256 (79-octet frame integrity protection)

Table C-12 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-14. Details of the computation follow the table.

Table C-16—GCM-AES-256 Key and calculated ICV (example)

Field	Value
Key (SAK)	4C973DBC7364621674F8B5B89E5C1551 1FCED9216490FB1C1A2CAA0FFE0407E5
ICV	00 BD A1 B7 E8 76 08 BC BF 47 0F 12 15 7F 4C 07

```
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:    7AE8E2CA4EC500012E58495C
GCM-AES Authentication
H:     9A5E559A96459C21E43C0DFF0FA426F3
Y[0]:  7AE8E2CA4EC500012E58495C00000001
E(K,Y[0]): 316F5EDB0829AC9271A6AFF79F3600BF
X[1]:  06A9019B44B76FFEC18978E8B21513E2
X[2]:  89A6401E39EAB6EE5B8159570139F54D
X[3]:  0A5E22BA54F282CE464C334D1AF598EF
X[4]: 4514D8A5C15E15CABC3D2A0E24FC758E
X[5]: 6F98DE3369B88F25AACBF3A993003E78
X[6]:  8183B21C0A932A2D5F598E1B2967564B
GHASH(H,A,C): 31D2FF6CE05FA42ECEE1A0E58A494CB8
C:
T: 00BDA1B7E87608BCBF470F12157F4C07
```

C.5 Confidentiality protection (54-octet frame)

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-17. 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-17—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-18.

Table C-18—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)
ICV	Cipher Suite and Key (SAK) dependent (see Table C-19 and Table C-20)

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-19 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-18. Details of the computation follow the table.

Table C-19—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-20 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-18. Details of the computation follow the table.

Table C-20—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.6 Confidentiality protection (60-octet frame)

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-21. 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-21—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-22.

Table C-22—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)
ICV	Cipher Suite and Key (SAK) dependent (see Table C-23 and Table C-24)

C.6.1 GCM-AES-128 (60-octet frame confidentiality protection)

Table C-23 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-22. Details of the computation follow the table.

Table C-23—GCM-AES-128 Key, Secure Data, and ICV (example)

Field	Value
Key (SAK)	AD7A2BD03EAC835A6F620FDCB506B345
Secure Data	70 1A FA 1C C0 39 C0 D7 65 12 8A 66 5D AB 69 24 38 99 BF 73 18 CC DC 81 C9 93 1D A1 7F BE 8E DD 7D 17 CB 8B 4C 26 FC 81 E3 28 4F 2B 7F BA 71 3D
ICV	4F 8D 55 E7 D3 F0 6F D5 A1 3C 0C 29 B9 D5 B8 80

```
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:    12153524C0895E81B2C28465

GCM-AES Encryption
H:            73A23D80121DE2D5A850253FCF43120E
Y[0]:         12153524C0895E81B2C2846500000001
E(K,Y[0]):    EB4E051CB548A6B5490F6F11A27CB7D0
Y[1]:         12153524C0895E81B2C2846500000002
E(K,Y[1]):    781AF50CD12BD3C370049D7E44B17238
C[1]:         701AFA1CC039C0D765128A665DAB6924
Y[2]:         12153524C0895E81B2C2846500000003
E(K,Y[2]):    2587A05339EEFFA5ECB53A895694A5F1
C[2]:         3899BF7318CCDC81C9931DA17FBE8EDD
Y[3]:         12153524C0895E81B2C2846500000004
E(K,Y[3]):    5039E4BB7D14CFB5D61E78134680713F
C[3]:         7D17CB8B4C26FC81E3284F2B7FBA713D
X[1]:         9CABBD91899C1413AA7AD629C1DF12CD
X[2]:         B99ABF6BDBD18B8E148F8030F0686F28
X[3]:         8B5BD74B9A65A459150392C3872BCE7F
X[4]:         934E9D58C59230EE652675D0FF4FB255
X[5]:         4738D208B10FAFF24D6DFBDDC916DC44
GHASH(H,A,C): A4C350FB66B8C960E83363381BA90F50

C:     701AFA1CC039C0D765128A665DAB6924
       3899BF7318CCDC81C9931DA17FBE8EDD
       7D17CB8B4C26FC81E3284F2B7FBA713D

T:     4F8D55E7D3F06FD5A13C0C29B9D5B880
```

C.6.2 GCM-AES-256 (60-octet frame confidentiality protection)

Table C-24 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-22. Details of the computation follow the table.

Table C-24—GCM-AES-256 Key, Secure Data, and ICV (example)

Field	Value
Key (SAK)	E3C08A8F06C6E3AD95A70557B23F7548 3CE33021A9C72B7025666204C69C0B72
Secure Data	E2 00 6E B4 2F 52 77 02 2D 9B 19 92 5B C4 19 D7 A5 92 66 6C 92 5F E2 EF 71 8E B4 E3 08 EF EA A7 C5 27 3B 39 41 18 86 0A 5B E2 A9 7F 56 AB 78 36
ICV	5C A5 97 CD BB 3E DB 8D 1A 11 51 EA 0A F7 B4 36

```
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:    12153524C0895E81B2C28465

GCM-AES Encryption
H:            286D73994EA0BA3CFD1F52BF06A8ACF2
Y[0]:         12153524C0895E81B2C2846500000001
E(K,Y[0]):    714D54FDCFCEE37D5729CDDAB383A016
Y[1]:         12153524C0895E81B2C2846500000002
E(K,Y[1]):    EA0061A43E406416388D0E8A42DE02CB
C[1]:         E2006EB42F5277022D9B19925BC419D7
Y[2]:         12153524C0895E81B2C2846500000003
E(K,Y[2]):    B88C794CB37DC1CB54A893CB21C5C18B
C[2]:         A592666C925FE2EF718EB4E308EFEAA7
Y[3]:         12153524C0895E81B2C2846500000004
E(K,Y[3]):    E8091409702AB53E6ED49E476F917834
C[3]:         C5273B394118860A5BE2A97F56AB7836
X[1]:         D62D2B0792C282A27B82C3731ABCB7A1
X[2]:         841068CDEDA878030E644F03743927D0
X[3]:         224CE5247BE62FB2AC5932EFAC5D1991
X[4]:         EB66718E589AB6472880D1A2C908CB72
X[5]:         6D109A3C7F34085754FDDFF0EB5D4595
GHASH(H,A,C): 2DE8C33074F038F04D389C30B9741420

C:     E2006EB42F5277022D9B19925BC419D7
       A592666C925FE2EF718EB4E308EFEAA7
       C5273B394118860A5BE2A97F56AB7836

T:     5CA597CDBB3EDB8D1A1151EA0AF7B436
```


C.7 Confidentiality protection (61-octet frame)

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	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-26.

Table C-26—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 C-27 and Table C-28)
ICV	Cipher Suite and Key (SAK) dependent (see Table C-27 and Table C-28)

C.7.1 GCM-AES-128 (61-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-26. Details of the computation follow the table.

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

Field	Value
Key (SAK)	013FE00B5F11BE7F866D0CBBC55A7A90
Secure Data	3A 4D E6 FA 32 19 10 14 DB B3 03 D9 2E E3 A9 E8 A1 B5 99 C1 4D 22 FB 08 00 96 E1 38 11 81 6A 3C 9C 9B CF 7C 1B 9B 96 DA 80 92 04 E2 9D 0E 2A 76 42
ICV	BF D3 10 A4 83 7C 81 6C CF A5 AC 23 AB 00 39 88

```
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:     7CFDE9F9E33724C68932D612
GCM-AES Encryption
H:            EB28DCB361EE1110F98CA0C9A07C88F7
Y[0]:         7CFDE9F9E33724C68932D61200000001
E(K,Y[0]):    4EAAF8E4DF948ACAC7F3349C1006A91F
Y[1]:         7CFDE9F9E33724C68932D61200000002
E(K,Y[1]):    324DE9EA230B0300CEA514C137F9B2F4
C[1]:         3A4DE6FA32191014DBB303D92EE3A9E8
Y[2]:         7CFDE9F9E33724C68932D61200000003
E(K,Y[2]):    BCAB86E16C00D82C25B0C61038AB4110
C[2]:         A1B599C14D22FB080096E13811816A3C
Y[3]:         7CFDE9F9E33724C68932D61200000004
E(K,Y[3]):    B1B5E04C2AA9A5EEB5A433DAA4341176
C[3]:         9C9BCF7C1B9B96DA809204E29D0E2A76
Y[4]:         7CFDE9F9E33724C68932D61200000005
E(K,Y[4]):    44491285F0FCF957EB73F79AC5D4E273
C[4]:         42
X[1]:         BA7749648FCB954F95B5933AC87D5AA3
X[2]:         A78C78463850956BF8939E6D8314DED1
X[3]:         18EB5A2C2541C14DD668468C26D2CD8A
X[4]:         32C49AA9AD2B7025767B14F37740A2E8
X[5]:         59CEE3A487F7ACAA9531883B31B11561
X[6]:         3FC125EEEC404708A0D8B9998FE0DE9B
GHASH(H,A,C): F179E8405CE80BA6085698BFBB069097
C:      3A4DE6FA32191014DBB303D92EE3A9E8
        A1B599C14D22FB080096E13811816A3C
        9C9BCF7C1B9B96DA809204E29D0E2A76
        42
T:      BFD310A4837C816CCFA5AC23AB003988
```


C.7.2 GCM-AES-256 (61-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-26. Details of the computation follow the table.

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

Field	Value
Key (SAK)	83C093B58DE7FFE1C0DA926AC43FB360 9AC1C80FEE1B624497EF942E2F79A823
Secure Data	11 02 22 FF 80 50 CB EC E6 6A 81 3A D0 9A 73 ED 7A 9A 08 9C 10 6B 95 93 89 16 8E D6 E8 69 8E A9 02 EB 12 77 DB EC 2E 68 E4 73 15 5A 15 A7 DA EE D4
ICV	A1 0F 4E 05 13 9C 23 DF 00 B3 AA DC 71 F0 59 6A

```
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:     7CFDE9F9E33724C68932D612
GCM-AES Encryption
H:             D03D3B51FDF2AACB3A165D7DC362D929
Y[0]:          7CFDE9F9E33724C68932D61200000001
E(K,Y[0]):     E97EA8EE4455AE79EC4225CAC340E326
Y[1]:          7CFDE9F9E33724C68932D61200000002
E(K,Y[1]):     19022DEF9142D8F8F37C9622C98068F1
C[1]:          110222FF8050CBECE66A813AD09A73ED
Y[2]:          7CFDE9F9E33724C68932D61200000003
E(K,Y[2]):     678417BC3149B6B7AC30A9FEC143A585
C[2]:          7A9A089C106B959389168ED6E8698EA9
Y[3]:          7CFDE9F9E33724C68932D61200000004
E(K,Y[3]):     2FC53D47EADE1D5CD14522622C9DE1EE
C[3]:          02EB1277DBEC2E68E473155A15A7DAEE
Y[4]:          7CFDE9F9E33724C68932D61200000005
E(K,Y[4]):     D2541F9E6E5ABAB19C0341912287646B
C[4]:          D4
X[1]:          0B75EC495656426640FD4E24ABA3ED1E
X[2]:          4BC3618F5864A86E9F4EE84504DE347C
X[3]:          F67E393EC69D2D6FFD54C4EFA6F5FF88
X[4]:          C7FE302C946CC29D1EFAAA22B7F587DD
X[5]:          87FCCA374A2EAFC6FD08FE08F919FB8E
X[6]:          0A648461F8E051A0B03165459D5E6F59
GHASH(H,A,C): 4871E6EB57C98DA6ECF18F16B2B0BA4C
C:      110222FF8050CBECE66A813AD09A73ED
        7A9A089C106B959389168ED6E8698EA9
        02EB1277DBEC2E68E473155A15A7DAEE
        D4
T:      A10F4E05139C23DF00B3AADC71F0596A
```


C.8 Confidentiality protection (75-octet frame)

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-29. 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-29—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-30.

Table C-30—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)
ICV	Cipher Suite and Key (SAK) dependent (see Table C-31 and Table C-32)

C.8.1 GCM-AES-128 (75-octet frame confidentiality protection)

Table C-31 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-30. Details of the computation follow the table.

Table C-31—GCM-AES-128 Key, Secure Data, and ICV (example)

Field	Value
Key (SAK)	88EE087FD95DA9FBF6725AA9D757B0CD
Secure Data	C3 1F 53 D9 9E 56 87 F7 36 51 19 B8 32 D2 AA E7 07 41 D5 93 F1 F9 E2 AB 34 55 77 9B 07 8E B8 FE AC DF EC 1F 8E 3E 52 77 F8 18 0B 43 36 1F 65 12 AD B1 6D 2E 38 54 8A 2C 71 9D BA 72 28 D8 40
ICV	88 F8 75 7A DB 8A A7 88 D8 F6 5A D6 68 BE 70 E7

```
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:    7AE8E2CA4EC500012E58495C
GCM-AES Encryption
H:            AE19118C3B704FCE42AE0D15D2C15C7A
Y[0]:         7AE8E2CA4EC500012E58495C00000001
E(K,Y[0]):    D2521AABC48C06033E112424D4A6DF74
Y[1]:         7AE8E2CA4EC500012E58495C00000002
E(K,Y[1]):    CB1F5CC98F4494E323470EA02BC8B1FB
C[1]:         C31F53D99E5687F7365119B832D2AAE7
Y[2]:         7AE8E2CA4EC500012E58495C00000003
E(K,Y[2]):    1A5FCAB3D0DBC18F117350B32EA493D2
C[2]:         0741D593F1F9E2AB3455779B078EB8FE
Y[3]:         7AE8E2CA4EC500012E58495C00000004
E(K,Y[3]):    81F1C32FBF0C6143CD2E3C7B0F255E2E
C[3]:         ACDFEC1F8E3E5277F8180B43361F6512
Y[4]:         7AE8E2CA4EC500012E58495C00000005
E(K,Y[4]):    908F526E7916C96834DBFD3A61D848B2
C[4]:         ADB16D2E38548A2C719DBA7228D840
X[1]:         A9845CAED3E164079E217A8D26A600DA
X[2]:         09410740B1204002F754119A976F31C8
X[3]:         CB897D3B71442B121E77CEA5416D3931
X[4]:         5F3A6A2D049FF2337096523ECAA1BD30
X[5]:         0C95908AEEBDAF1B1C279837AE498000
X[6]:         1ACA99E1E46D2395BC610D21BB4216A0
GHASH(H,A,C): 5AAA6FD11F06A18BE6E77EF2BC18AF93
C:     C31F53D99E5687F7365119B832D2AAE7
       0741D593F1F9E2AB3455779B078EB8FE
       ACDFEC1F8E3E5277F8180B43361F6512
       ADB16D2E38548A2C719DBA7228D840
T:     88F8757ADB8AA788D8F65AD668BE70E7
```

C.8.2 GCM-AES-256 (75-octet frame confidentiality protection)

Table C-32 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-30. Details of the computation follow the table.

Table C-32—GCM-AES-256 Key, Secure Data, and ICV (example)

Field	Value
Key (SAK)	4C973DBC7364621674F8B5B89E5C1551 1FCED9216490FB1C1A2CAA0FFE0407E5
Secure Data	BA 8A E3 1B C5 06 48 6D 68 73 E4 FC E4 60 E7 DC 57 59 1F F0 06 11 F3 1C 38 34 FE 1C 04 AD 80 B6 68 03 AF CF 5B 27 E6 33 3F A6 7C 99 DA 47 C2 F0 CE D6 8D 53 1B D7 41 A9 43 CF F7 A6 71 3B D0
ICV	26 11 CD 7D AA 01 D6 1C 5C 88 6D C1 A8 17 01 07

```
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:     7AE8E2CA4EC500012E58495C
GCM-AES Encryption
H:             9A5E559A96459C21E43C0DFF0FA426F3
Y[0]:          7AE8E2CA4EC500012E58495C00000001
E(K,Y[0]):     316F5EDB0829AC9271A6AFF79F3600BF
Y[1]:          7AE8E2CA4EC500012E58495C00000002
E(K,Y[1]):     B28AEC0BD4145B797D65F3E4FD7AFCC0
C[1]:          BA8AE31BC506486D6873E4FCE460E7DC
Y[2]:          7AE8E2CA4EC500012E58495C00000003
E(K,Y[2]):     4A4700D02733D0381D12D9342D87AB9A
C[2]:          57591FF00611F31C3834FE1C04AD80B6
Y[3]:          7AE8E2CA4EC500012E58495C00000004
E(K,Y[3]):     452D80FF6A15D5070A904BA1E37DF9CC
C[3]:          6803AFCF5B27E6333FA67C99DA47C2F0
Y[4]:          7AE8E2CA4EC500012E58495C00000005
E(K,Y[4]):     F3E8B2135A9502ED0689B0EE383BD81D
C[4]:          CED68D531BD741A943CFF7A6713BD0
X[1]:          1F7477283AA77457BD0C161CB6F179C5
X[2]:          617F112B72DF67BC42218163B73AF025
X[3]:          20A91ADD33433324DBE7822A5BC98013
X[4]:          84D320FCB3B7AF10A66A48BADD00CFA1
X[5]:          52F52D34BC031431185DB9A617FCE98C
X[6]:          57E7CFDDBA0BA07415FD58BCEE906CAC
GHASH(H,A,C): 177E93A6A2287A8E2D2EC236372101B8
C:      BA8AE31BC506486D6873E4FCE460E7DC
        57591FF00611F31C3834FE1C04AD80B6
        6803AFCF5B27E6333FA67C99DA47C2F0
        CED68D531BD741A943CFF7A6713BD0
T:      2611CD7DAA01D61C5C886DC1A8170107
```