

# ISO/IEC/IEEE 8802-1AE AMD 1:2015-05 (E)

## Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Part 1AE: Media access control (MAC) security - Amendment 1: Galois Counter Mode - Advanced Encryption Standard-256 (GCM-AES-256) Cipher Suite

---

<b>Contents</b>	<b>Page</b>
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