

ISO/IEC/IEEE 8802-1AE:2013-12 (E)

Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Part 1AE: Media access control (MAC) security

Contents

- 1. Overview 1
 - 1.1 Introduction 1
 - 1.2 Scope 2
- 2. Normative references 3
- 3. Definitions 5
- 4. Abbreviations and acronyms 8
- 5. Conformance 10
 - 5.1 Requirements terminology 10
 - 5.2 Protocol Implementation Conformance Statement (PICS) 10
 - 5.3 Required capabilities 10
 - 5.4 Optional capabilities 11
- 6. Secure provision of the MAC Service 13
 - 6.1 MAC Service primitives and parameters 13
 - 6.2 MAC Service connectivity 15
 - 6.3 Point-to-multipoint LANs 16
 - 6.4 MAC status parameters 16
 - 6.5 MAC point-to-point parameters 16
 - 6.6 Security threats 17
 - 6.7 MACsec connectivity 18
 - 6.8 MACsec guarantees 19
 - 6.9 Security services 19
 - 6.10 Quality of service maintenance 20
- 7. Principles of secure network operation 22
 - 7.1 Support of the secure MAC Service by an individual LAN 22
 - 7.2 Multiple instances of the secure MAC Service on a single LAN 27
 - 7.3 Use of the secure MAC Service 28
- 8. MAC Security Protocol (MACsec) 31
 - 8.1 Protocol design requirements 32
 - 8.2 Protocol support requirements 34
 - 8.3 MACsec operation 36
- 9. Encoding of MACsec protocol data units 38
 - 9.1 Structure, representation, and encoding 38
 - 9.2 Major components 38
 - 9.3 Security TAG 39
 - 9.4 MACsec EtherType 39
 - 9.5 TAG Control Information (TCI) 40
 - 9.6 Association Number (AN) 41
 - 9.7 Short Length (SL) 41
 - 9.8 Packet Number (PN) 41
 - 9.9 Secure Channel Identifier (SCI) 41
 - 9.10 Secure Data 42

9.11	Integrity Check Value (ICV)	42
9.12	PDU validation	43
10.	Principles of MAC Security Entity (SecY) operation	44
10.1	SecY overview	44
10.2	SecY functions	46
10.3	Model of operation	47
10.4	SecY architecture	47
10.5	Secure frame generation	50
10.6	Secure frame verification	51
10.7	SecY management	53
10.8	Addressing	63
10.9	Priority	63
10.10	SecY performance requirements	63
11.	MAC Security in Systems	65
11.1	MAC Service interface stacks	65
11.2	MACsec in end stations	66
11.3	MACsec in MAC Bridges	66
11.4	MACsec in VLAN-aware Bridges	67
11.5	MACsec and Link Aggregation	68
11.6	Link Layer Discovery Protocol (LLDP)	69
11.7	MACsec in Provider Bridged Networks	70
11.8	MACsec and multi-access LANs	72
12.	MACsec and EPON	74
13.	Management protocol	76
13.1	Introduction	76
13.2	The Internet-Standard Management Framework	76
13.3	Relationship to other MIBs	76
13.4	Security considerations	78
13.5	Structure of the MIB	80
13.6	Definitions for MAC Security MIB	84
14.	Cipher Suites	121
14.1	Cipher Suite use	121
14.2	Cipher Suite capabilities	122
14.3	Cipher Suite specification	123
14.4	Cipher Suite conformance	123
14.5	Default Cipher Suite (GCM–AES–128)	124
Annex A	(normative) PICS Proforma	126
A.1	Introduction	126
A.2	Abbreviations and special symbols	126
A.3	Instructions for completing the PICS proforma	127
A.4	PICS proforma for IEEE Std 802.1AE	129
A.5	Major capabilities	130
A.6	Support and use of Service Access Points	131
A.7	MAC status and point-to-point parameters	132
A.8	Secure Frame Generation	133

A.9	Secure Frame Verification	134
A.10	MACsec PDU encoding and decoding	135
A.11	Key Agreement Entity LMI	135
A.12	Additional fully conformant Cipher Suite capabilities	139
A.13	Additional variant Cipher Suite capabilities	140
Annex B (informative) Bibliography		142
Annex E (informative) KGK"hu"qh'r ct vkr cpvu"		145