

ISO/IEC/IEEE 8802-1AE:2020-08 (E)

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

Contents

- 1. Overview 16
 - 1.1 Introduction 16
 - 1.2 Scope 17
- 2. Normative references 18
- 3. Definitions 19
- 4. Abbreviations and acronyms 23
- 5. Conformance 25
 - 5.1 Requirements terminology 25
 - 5.2 Protocol Implementation Conformance Statement (PICS) 25
 - 5.3 MAC Security Entity requirements 26
 - 5.4 MAC Security Entity options 27
 - 5.5 EDE conformance 27
 - 5.6 EDE-M conformance 28
 - 5.7 EDE-CS conformance 28
 - 5.8 EDE-CC conformance 29
 - 5.9 EDE-SS conformance 29
- 6. Secure provision of the MAC Service 30
 - 6.1 MAC Service primitives and parameters 30
 - 6.2 MAC Service connectivity 32
 - 6.3 Point-to-multipoint LANs 32
 - 6.4 MAC status parameters 33
 - 6.5 MAC point-to-point parameters 33
 - 6.6 Security threats 34
 - 6.7 MACsec connectivity 35
 - 6.8 MACsec guarantees 35
 - 6.9 Security services 36
 - 6.10 Quality of Service maintenance 37
- 7. Principles of secure network operation 39
 - 7.1 Support of the secure MAC Service by an individual LAN 39
 - 7.2 Multiple instances of the secure MAC Service on a single LAN 44
 - 7.3 Use of the secure MAC Service 45
- 8. MAC Security protocol (MACsec) 48
 - 8.1 Protocol design requirements 48
 - 8.2 Protocol support requirements 51
 - 8.3 MACsec operation 53
- 9. Encoding of MACsec Protocol Data Units 55
 - 9.1 Structure, representation, and encoding 55
 - 9.2 Major components 55
 - 9.3 MAC Security TAG 56
 - 9.4 MACsec EtherType 56

| | | |
|-------|---|-----|
| 9.5 | TAG Control Information (TCI)..... | 57 |
| 9.6 | Association Number (AN)..... | 58 |
| 9.7 | Short Length (SL)..... | 58 |
| 9.8 | Packet Number (PN)..... | 58 |
| 9.9 | Secure Channel Identifier (SCI)..... | 59 |
| 9.10 | Secure Data..... | 59 |
| 9.11 | Integrity check value (ICV)..... | 59 |
| 9.12 | PDU validation..... | 60 |
| 10. | Principles of MAC Security Entity (SecY) operation..... | 61 |
| 10.1 | SecY overview..... | 61 |
| 10.2 | SecY functions..... | 62 |
| 10.3 | Model of operation..... | 63 |
| 10.4 | SecY architecture..... | 63 |
| 10.5 | Secure frame generation..... | 65 |
| 10.6 | Secure frame verification..... | 68 |
| 10.7 | SecY management..... | 72 |
| 10.8 | Addressing..... | 85 |
| 10.9 | Priority..... | 85 |
| 10.10 | SecY performance requirements..... | 86 |
| 11. | MAC Security in systems..... | 87 |
| 11.1 | MAC Service interface stacks..... | 87 |
| 11.2 | MACsec in end stations..... | 88 |
| 11.3 | MACsec in MAC Bridges..... | 89 |
| 11.4 | MACsec in VLAN-aware Bridges..... | 90 |
| 11.5 | MACsec and Link Aggregation..... | 91 |
| 11.6 | Link Layer Discovery Protocol (LLDP)..... | 92 |
| 11.7 | MACsec in Provider Bridged Networks..... | 93 |
| 11.8 | MACsec and multi-access LANs..... | 95 |
| 12. | MACsec and EPON..... | 97 |
| 13. | MAC Security Entity MIB..... | 98 |
| 13.1 | Introduction..... | 98 |
| 13.2 | The Internet-Standard Management Framework..... | 98 |
| 13.3 | Relationship to other MIBs..... | 98 |
| 13.4 | Security considerations..... | 100 |
| 13.5 | Structure of the MIB module..... | 102 |
| 13.6 | MAC Security Entity (SecY) MIB definitions..... | 107 |
| 14. | Cipher Suites..... | 141 |
| 14.1 | Cipher Suite use..... | 141 |
| 14.2 | Cipher Suite capabilities..... | 142 |
| 14.3 | Cipher Suite specification..... | 143 |
| 14.4 | Cipher Suite conformance..... | 143 |
| 14.5 | Default Cipher Suite (GCM-AES-128)..... | 145 |
| 14.6 | GCM-AES-256..... | 146 |
| 14.7 | GCM-AES-XPN-128..... | 147 |
| 14.8 | GCM-AES-XPN-256..... | 148 |

| | | |
|---------|---|-----|
| 15. | Ethernet Data Encryption devices..... | 149 |
| 15.1 | EDE characteristics..... | 149 |
| 15.2 | Securing LANs with EDE-Ms..... | 150 |
| 15.3 | Securing connectivity across PBNs..... | 152 |
| 15.4 | Securing PBN connectivity with an EDE-M..... | 153 |
| 15.5 | Securing PBN connectivity with an EDE-CS..... | 154 |
| 15.6 | Securing PBN connectivity with an EDE-CC..... | 156 |
| 15.7 | Securing PBN connectivity with an EDE-SS..... | 158 |
| 15.8 | EDE Interoperability..... | 159 |
| 15.9 | EDEs, CFM, and UNI Access..... | 160 |
| 16. | Using MIB modules to manage EDEs..... | 161 |
| 16.1 | Security considerations..... | 161 |
| 16.2 | EDE-M Management..... | 161 |
| 16.3 | EDE-CS Management..... | 161 |
| 16.4 | EDE-CC and EDE-SS Management..... | 161 |
| Annex A | (normative) PICS proforma..... | 163 |
| A.1 | Introduction..... | 163 |
| A.2 | Abbreviations and special symbols..... | 163 |
| A.3 | Instructions for completing the PICS proforma..... | 164 |
| A.4 | PICS proforma for IEEE Std 802.1AE..... | 166 |
| A.5 | Major capabilities..... | 167 |
| A.7 | MAC status and point-to-point parameters..... | 169 |
| A.6 | Support and use of Service Access Points..... | 169 |
| A.8 | Secure Frame Generation..... | 170 |
| A.9 | Secure Frame Verification..... | 171 |
| A.10 | MACsec PDU encoding and decoding..... | 172 |
| A.11 | Key Agreement Entity LMI..... | 172 |
| A.12 | Management..... | 173 |
| A.13 | Additional fully conformant Cipher Suite capabilities..... | 177 |
| A.14 | Additional variant Cipher Suite capabilities..... | 177 |
| Annex B | (informative) Bibliography..... | 180 |
| Annex C | (informative) MACsec test vectors..... | 182 |
| C.1 | Integrity protection (54-octet frame)..... | 183 |
| C.2 | Integrity protection (60-octet frame)..... | 188 |
| C.3 | Integrity protection (65-octet frame)..... | 193 |
| C.4 | Integrity protection (79-octet frame)..... | 198 |
| C.5 | Confidentiality protection (54-octet frame)..... | 203 |
| C.6 | Confidentiality protection (60-octet frame)..... | 208 |
| C.7 | Confidentiality protection (61-octet frame)..... | 213 |
| C.8 | Confidentiality protection (75-octet frame)..... | 218 |
| Annex D | (normative) PICS proforma for an Ethernet Data Encryption device..... | 223 |
| D.1 | Introduction..... | 223 |
| D.2 | Abbreviations and special symbols..... | 223 |
| D.3 | Instructions for completing the PICS proforma..... | 224 |
| D.4 | PICS proforma for IEEE Std 802.1AE EDE..... | 226 |
| D.5 | EDE type and common requirements..... | 227 |

| | | |
|---|-------------------------------|-----|
| D.6 | EDE-M Configuration | 228 |
| D.7 | EDE-CS Configuration | 229 |
| D.8 | EDE-CC Configuration..... | 229 |
| D.9 | EDE-SS Configuration | 229 |
| Annex E (informative) MKA operation for multiple transmit SCs | | 230 |
| Annex F (informative) EDE Interoperability and PAE addresses | | 232 |
| Annex G (informative) Management and MIB revisions | | 235 |
| G.1 | Counter changes..... | 236 |
| G.2 | Available Cipher Suites | 237 |

Figures

| | | |
|--------------|--|-----|
| Figure 6-1 | MACsec secured LAN with three stations..... | 30 |
| Figure 6-2 | MACsec Frame, VLAN TAG, and QoS..... | 32 |
| Figure 7-1 | Two stations connected by a point-to-point LAN..... | 40 |
| Figure 7-2 | Two stations in a CA created by MACsec Key Agreement | 40 |
| Figure 7-3 | Secure communication between two stations | 41 |
| Figure 7-4 | Four stations attached to a shared media LAN | 41 |
| Figure 7-5 | A CA including ports A, B, and C | 42 |
| Figure 7-6 | Secure communication between three stations | 42 |
| Figure 7-7 | Secure Channel and Secure Association Identifiers | 44 |
| Figure 8-1 | MACsec | 48 |
| Figure 8-2 | MACsec operation | 54 |
| Figure 9-1 | MPDU components..... | 56 |
| Figure 9-2 | SecTAG format..... | 56 |
| Figure 9-3 | MACsec EtherType encoding..... | 57 |
| Figure 9-4 | MACsec TCI and AN Encoding..... | 57 |
| Figure 10-1 | SecY | 61 |
| Figure 10-2 | SecY architecture and operation | 64 |
| Figure 10-3 | Management controls and counters for secure frame generation | 66 |
| Figure 10-4 | Management controls and counters for secure frame verification..... | 69 |
| Figure 10-5 | SecY managed objects | 73 |
| Figure 11-1 | Direct support of the MAC Service by a media access method..... | 87 |
| Figure 11-2 | Provision of MAC Service with media-independent functions | 88 |
| Figure 11-3 | MACsec in an end station | 88 |
| Figure 11-4 | MACsec in a VLAN-unaware MAC Bridge..... | 89 |
| Figure 11-5 | VLAN-unaware MAC Bridge Port with MACsec..... | 89 |
| Figure 11-6 | Addition of MAC Security to a VLAN-aware MAC Bridge..... | 90 |
| Figure 11-7 | IEEE 802.1Q VLAN-aware Bridge Port with MACsec | 90 |
| Figure 11-8 | MACsec and Link Aggregation in an interface stack..... | 91 |
| Figure 11-9 | IEEE 802.1Q VLAN-aware Bridge Port with MACsec and Link Aggregation | 92 |
| Figure 11-10 | MACsec with LLDP | 92 |
| Figure 11-11 | Internal organization of the MAC sublayer in a Provider Bridged Network..... | 93 |
| Figure 11-12 | Interface stack for MAC Security to and across provider's network..... | 93 |
| Figure 11-13 | Provider network with priority selection and aggregation..... | 94 |
| Figure 11-14 | An example multi-access LAN | 95 |
| Figure 11-15 | Multi-access LAN interface stack..... | 96 |
| Figure 12-1 | MACsec with EPON, showing SCs and SCB..... | 97 |
| Figure 13-1 | MACsec Interface Stack | 98 |
| Figure 13-2 | SecY MIB structure..... | 103 |
| Figure 14-1 | Cipher Suite Protect and Validate operations | 141 |
| Figure 15-1 | EDE-Ms connected by a point-to-point LAN | 150 |
| Figure 15-2 | EDE-Ms securing a point-to-point LAN between Provider Bridges | 151 |
| Figure 15-3 | MACsec protected frame traversing a PBN..... | 152 |
| Figure 15-4 | EDE-Ms securing point-to-point LAN connectivity across a PBN | 153 |
| Figure 15-5 | EDE-Ms securing multi-point PBN connectivity | 154 |
| Figure 15-6 | Example network with an EDE-CS | 155 |
| Figure 15-7 | EDE-CS connected to a PBN S-tagged interface..... | 156 |
| Figure 15-8 | Using an EDE-CC with a C-tagged provider service interface | 157 |
| Figure 15-9 | EDE-CC architecture | 158 |

Tables

| | | |
|------------|---|-----|
| Table 9-1 | MACsec EtherType allocation..... | 56 |
| Table 10-1 | Management controls and SecTAG encoding | 67 |
| Table 10-2 | Extended packet number recovery (examples)..... | 70 |
| Table 10-3 | SecY performance requirements..... | 86 |
| Table 13-1 | Use of ifGeneralInformationGroup Objects | 99 |
| Table 13-2 | Use of ifCounterDiscontinuityGroup Object | 100 |
| Table 13-3 | Use of ifStackTable | 100 |
| Table 13-4 | Use of ifStackGroup2 Objects | 100 |
| Table 13-5 | Controlled Port service management..... | 104 |
| Table 13-6 | Transmit and receive SC management | 105 |
| Table 13-7 | Transmit and receive statistics..... | 106 |
| Table 13-8 | Cipher Suite information | 107 |
| Table 14-1 | MACsec Cipher Suites..... | 144 |
| Table 15-1 | PAE Group Addresses | 159 |
| Table 15-2 | PAE Group Address use | 160 |
| Table C-1 | Unprotected frame (example)..... | 183 |
| Table C-2 | Integrity protected frame (example)..... | 183 |
| Table C-3 | GCM-AES-128 Key and calculated ICV (example) | 184 |
| Table C-4 | GCM-AES-256 Key and calculated ICV (example) | 185 |
| Table C-5 | GCM-AES-XPEN-128 Key and calculated ICV (example)..... | 186 |
| Table C-6 | GCM-AES-XPEN-256 Key and calculated ICV (example)..... | 187 |
| Table C-7 | Unprotected frame (example)..... | 188 |
| Table C-8 | Integrity protected frame (example)..... | 188 |
| Table C-9 | GCM-AES-128 Key and calculated ICV (example) | 189 |
| Table C-10 | GCM-AES-256 Key and calculated ICV (example) | 190 |
| Table C-11 | GCM-AES-XPEN-128 Key and calculated ICV (example)..... | 191 |
| Table C-12 | GCM-AES-XPEN-256 Key and calculated ICV (example)..... | 192 |
| Table C-13 | Unprotected frame (example)..... | 193 |
| Table C-14 | Integrity protected frame (example)..... | 193 |
| Table C-15 | GCM-AES-128 Key and calculated ICV (example) | 194 |
| Table C-16 | GCM-AES-256 Key and calculated ICV (example) | 195 |
| Table C-17 | GCM-AES-XPEN-128 Key and calculated ICV (example)..... | 196 |
| Table C-18 | GCM-AES-XPEN-256 Key and calculated ICV (example)..... | 197 |
| Table C-19 | Unprotected frame (example)..... | 198 |
| Table C-20 | Integrity protected frame (example)..... | 198 |
| Table C-21 | GCM-AES-128 Key and calculated ICV (example) | 199 |
| Table C-22 | GCM-AES-256 Key and calculated ICV (example) | 200 |
| Table C-23 | GCM-AES-XPEN-128 Key and calculated ICV (example)..... | 201 |
| Table C-24 | GCM-AES-XPEN-256 Key and calculated ICV (example)..... | 202 |
| Table C-25 | Unprotected frame (example)..... | 203 |
| Table C-26 | Confidentiality protected frame (example)..... | 203 |
| Table C-27 | GCM-AES-128 Key, Secure Data, and ICV (example)..... | 204 |
| Table C-28 | GCM-AES-256 Key, Secure Data, and ICV (example)..... | 205 |
| Table C-29 | GCM-AES-XPEN-128 Key, Secure Data, and ICV (example)..... | 206 |
| Table C-30 | GCM-AES-XPEN-256 Key, Secure Data, and ICV (example)..... | 207 |
| Table C-31 | Unprotected frame (example)..... | 208 |
| Table C-32 | Confidentiality protected frame (example)..... | 208 |
| Table C-33 | GCM-AES-128 Key, Secure Data, and ICV (example)..... | 209 |
| Table C-34 | GCM-AES-256 Key, Secure Data, and ICV (example)..... | 210 |
| Table C-35 | GCM-AES-XPEN-128 Key, Secure Data, and ICV (example)..... | 211 |
| Table C-36 | GCM-AES-XPEN-256 Key, Secure Data, and ICV (example)..... | 212 |
| Table C-37 | Unprotected frame (example)..... | 213 |

| | | |
|------------|--|-----|
| Table C-38 | Confidentiality protected frame (example)..... | 213 |
| Table C-39 | GCM-AES-128 Key, Secure Data, and ICV (example)..... | 214 |
| Table C-40 | GCM-AES-256 Key, Secure Data, and ICV (example)..... | 215 |
| Table C-41 | GCM-AES-XPB-128 Key, Secure Data, and ICV (example)..... | 216 |
| Table C-42 | GCM-AES-XPB-256 Key, Secure Data, and ICV (example)..... | 217 |
| Table C-43 | Unprotected frame (example)..... | 218 |
| Table C-44 | Confidentiality protected frame (example)..... | 218 |
| Table C-45 | GCM-AES-128 Key, Secure Data, and ICV (example)..... | 219 |
| Table C-46 | GCM-AES-256 Key, Secure Data, and ICV (example)..... | 220 |
| Table C-47 | GCM-AES-XPB-128 Key, Secure Data, and ICV (example)..... | 221 |
| Table C-48 | GCM-AES-XPB-256 Key, Secure Data, and ICV (example)..... | 222 |
| Table F-1 | Interoperability scenarios and PAE Addresses..... | 234 |