



International  
Standard

**ISO/IEC/IEEE  
8802-1AE**

**Telecommunications and exchange  
between information technology  
systems — Requirements for local  
and metropolitan area networks —**

**Part 1AE:  
Media access control (MAC) security**

**AMENDMENT 4: MAC Privacy  
Protection**

*Télécommunications et échange entre systèmes informatiques —  
Exigences pour les réseaux locaux et métropolitains —*

*Partie 1AE: Sécurité du contrôle d'accès aux supports (MAC)*

*AMENDEMENT 4: Protection de la vie privée MAC*

**Second edition  
2020-08**

**AMENDMENT 4  
2024-11**

Reference number  
ISO/IEC/IEEE 8802-1AE:2020/  
Amd.4:2024(en)

Full document details: ISO/IEC/IEEE 08802-1AE-2020 amd4-2024

© IEEE 2024



**Documents**  
Document Sharing Hub



**COPYRIGHT PROTECTED DOCUMENT**

© IEEE 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from IEEE at the address below.

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

Email: [stds.ipr@ieee.org](mailto:stds.ipr@ieee.org)  
Website: [www.ieee.org](http://www.ieee.org)

Published in Switzerland

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see [www.iso.org/directives](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs)).

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.

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at [www.iso.org/patents](http://www.iso.org/patents) and <https://patents.iec.ch>. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see [www.iso.org/iso/foreword.html](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://www.iec.ch/understanding-standards).

ISO/IEC/IEEE 8802-1AE:2020/Amd.4 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE Std 802.1AEdk-2023) and drafted in accordance with its editorial rules. It was adopted, under the "fast-track procedure" defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

A list of all parts in the ISO/IEC/IEEE 8802 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at [www.iso.org/members.html](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## Contents

|      |                                                                         |    |
|------|-------------------------------------------------------------------------|----|
| 1.   | Overview.....                                                           | 16 |
| 1.1  | Introduction.....                                                       | 16 |
| 1.2  | Scope.....                                                              | 17 |
| 2.   | Normative references.....                                               | 19 |
| 3.   | Definitions .....                                                       | 21 |
| 4.   | Abbreviations and acronyms .....                                        | 22 |
| 5.   | Conformance.....                                                        | 23 |
| 5.1  | Requirements terminology.....                                           | 23 |
| 5.2  | Protocol Implementation Conformance Statements (PICS) .....             | 24 |
| 5.5  | EDE Conformance .....                                                   | 24 |
| 5.8  | EDE-CC conformance .....                                                | 25 |
| 5.10 | MAC Privacy protection Entity requirements .....                        | 25 |
| 5.11 | MAC Privacy protection Entity options .....                             | 26 |
| 10.  | Principles of MAC Security Entity (SecY) operation .....                | 27 |
| 10.7 | SecY management .....                                                   | 27 |
| 13.  | MAC Security Entity MIB.....                                            | 30 |
| 13.1 | Introduction.....                                                       | 30 |
| 13.6 | MAC Security Entity (SecY) MIB definition, .....                        | 31 |
| 15.  | Ethernet Data Encryption devices.....                                   | 69 |
| 15.6 | Securing PBN connectivity with an EDE-CC .....                          | 69 |
| 16.  | Using MIB modules to manage EDEs.....                                   | 70 |
| 16.4 | EDE-CC and EDE-SS Management.....                                       | 70 |
| 17.  | MAC Privacy protection.....                                             | 71 |
| 17.1 | Need for MAC Privacy protection.....                                    | 71 |
| 17.2 | Protecting user data frames.....                                        | 72 |
| 17.3 | Quality of Service impact and mitigation .....                          | 74 |
| 17.4 | Configuring MAC Privacy protection .....                                | 76 |
| 18.  | MAC Privacy protection protocol.....                                    | 81 |
| 18.1 | Addressing .....                                                        | 81 |
| 18.2 | Data origin authenticity, frame data integrity and confidentiality..... | 82 |
| 18.3 | Applicability .....                                                     | 82 |
| 18.4 | Bandwidth utilization, fragmentation, and transit delay .....           | 83 |
| 18.5 | Coexistence and use.....                                                | 84 |
| 19.  | Encoding of MAC Privacy protection Protocol Data Units .....            | 85 |
| 19.1 | Structure, representation, and encoding.....                            | 85 |
| 19.2 | MPPDU Format .....                                                      | 85 |

|       |                                                         |     |
|-------|---------------------------------------------------------|-----|
| 19.3  | MAC Privacy protection EtherType .....                  | 86  |
| 19.4  | Protocol Version strategy.....                          | 87  |
| 19.5  | MPPDU component encoding .....                          | 87  |
| 19.6  | MPPDU generation.....                                   | 90  |
| 19.7  | MPPDU validation.....                                   | 91  |
| 20.   | MAC Privacy protection Entity (PrY) operation .....     | 93  |
| 20.1  | PrY overview .....                                      | 93  |
| 20.2  | Model of operation.....                                 | 94  |
| 20.3  | PrY architecture .....                                  | 94  |
| 20.4  | MAC status and point-to-point parameters.....           | 95  |
| 20.5  | Privacy Selection .....                                 | 95  |
| 20.6  | Unprotected frame transmission .....                    | 96  |
| 20.7  | Privacy Frame transmission.....                         | 96  |
| 20.8  | Privacy Channel transmission.....                       | 97  |
| 20.9  | Privacy Channel MPPDU Generation .....                  | 97  |
| 20.10 | Privacy Channel Encapsulation .....                     | 100 |
| 20.11 | MPPDU reception and demultiplexing.....                 | 101 |
| 20.12 | MPPDU component validation and extraction .....         | 103 |
| 20.13 | Protected frame reception and reassembly .....          | 103 |
| 20.14 | PrY management.....                                     | 106 |
| 20.15 | PrY performance requirements .....                      | 109 |
| 21.   | MAC Privacy protection in Systems .....                 | 110 |
| 21.1  | MAC Privacy protection interface stacks .....           | 110 |
| 21.2  | Privacy protection for end station interfaces .....     | 112 |
| 21.3  | MAC Privacy protection for bridge interfaces .....      | 112 |
| 21.4  | Privacy protection for Link Aggregation .....           | 113 |
| 21.5  | EDEs with MAC Privacy protection .....                  | 114 |
| 21.6  | Privacy protection with shared media.....               | 115 |
| 21.7  | Privacy protection and multi-access LANs .....          | 116 |
| 21.8  | Separate privacy protection devices .....               | 116 |
| 22.   | MAC Privacy protection Entity (Pry) MIB .....           | 117 |
| 22.1  | Introduction.....                                       | 117 |
| 22.2  | The Internet-Standard Management Framework .....        | 117 |
| 22.3  | Relationship to other MIBs.....                         | 117 |
| 22.4  | Security considerations .....                           | 119 |
| 22.5  | Structure of the MIB module.....                        | 120 |
| 23.   | YANG Data Models .....                                  | 139 |
| 23.1  | YANG Framework .....                                    | 140 |
| 23.2  | MAC Security Entity (SecY) model.....                   | 141 |
| 23.3  | Security considerations for the SecY model.....         | 145 |
| 23.4  | MAC Privacy protection (PrY) model.....                 | 146 |
| 23.5  | Security considerations for the PrY model.....          | 148 |
| 23.6  | Interface stack models .....                            | 149 |
| 23.7  | Security considerations for interface stack models..... | 151 |
| 23.8  | System models .....                                     | 151 |
| 23.9  | Security considerations for system models.....          | 152 |
| 23.10 | YANG module schema.....                                 | 153 |
| 23.11 | YANG modules .....                                      | 157 |

|                                                                                |     |
|--------------------------------------------------------------------------------|-----|
| Annex B (informative) Bibliography .....                                       | 186 |
| Annex D (normative) PICS Proforma for an Ethernet Data Encryption device ..... | 188 |
| D.5    EDE type and common requirements .....                                  | 188 |
| D.8    EDE-CC Configuration.....                                               | 189 |
| Annex G (informative) SecY Management and MIB revisions .....                  | 190 |
| Annex H (normative) PICS proforma for MAC Privacy protection .....             | 191 |
| H.1    Introduction.....                                                       | 191 |
| H.2    Abbreviations and special symbols.....                                  | 191 |
| H.3    Instructions for completing the PICS proforma.....                      | 192 |
| H.4    PICS proforma for IEEE Std 802.1AE MAC Privacy protection .....         | 194 |
| H.5    Mandatory capabilities.....                                             | 195 |
| H.6    Optional capabilities .....                                             | 196 |
| Annex I (informative) Privacy considerations in bridged networks .....         | 197 |
| I.1    Personal devices.....                                                   | 197 |
| I.2    Goals of adversaries .....                                              | 197 |
| I.3    Network operation .....                                                 | 198 |
| I.4    Network security and privacy .....                                      | 199 |
| I.5    Privacy exposures .....                                                 | 199 |
| I.6    Standard specific considerations.....                                   | 201 |

## Figures

|             |                                                                        |     |
|-------------|------------------------------------------------------------------------|-----|
| Figure 10-5 | SecY managed objects .....                                             | 28  |
| Figure 13-1 | MACsec Interface Stack .....                                           | 30  |
| Figure 17-1 | Privacy-protected communication between bridges .....                  | 73  |
| Figure 17-2 | A privacy protected user data frame .....                              | 73  |
| Figure 17-3 | Privacy selection, priority and traffic class mapping.....             | 80  |
| Figure 19-1 | MACsec protected MPPDU .....                                           | 85  |
| Figure 19-2 | MPPDU Examples .....                                                   | 86  |
| Figure 19-3 | MAC Privacy protection EtherType encoding.....                         | 87  |
| Figure 19-4 | MPPDU component format .....                                           | 87  |
| Figure 19-5 | MPPDU component encoding .....                                         | 88  |
| Figure 19-6 | Frame Fragments.....                                                   | 89  |
| Figure 20-1 | PrY and SecY .....                                                     | 93  |
| Figure 20-2 | PrY architecture .....                                                 | 94  |
| Figure 20-3 | Privacy Channel Encapsulation state machine.....                       | 102 |
| Figure 20-4 | Protected frame reception and reassembly.....                          | 104 |
| Figure 20-5 | Reassembly state machine .....                                         | 105 |
| Figure 20-6 | PrY Managed objects .....                                              | 107 |
| Figure 21-1 | A Privacy-protecting interface stack.....                              | 110 |
| Figure 21-2 | Privacy-protected Bridge Ports .....                                   | 112 |
| Figure 21-3 | Privacy protection and Link Aggregation.....                           | 113 |
| Figure 21-4 | EDE-CC with privacy-protection.....                                    | 114 |
| Figure 21-5 | EDE-CCs communicating over a PBN .....                                 | 114 |
| Figure 21-6 | Privacy-protection using existing EDEs .....                           | 116 |
| Figure 22-1 | PrY Interfaces .....                                                   | 117 |
| Figure 22-2 | PrY MIB structure.....                                                 | 121 |
| Figure 23-1 | YANG hierarchy, models and objects .....                               | 140 |
| Figure 23-2 | SecY model system nodes and references .....                           | 142 |
| Figure 23-3 | SecY model system nodes and references .....                           | 143 |
| Figure 23-4 | PrY model interface nodes .....                                        | 147 |
| Figure 23-5 | Explicit and augmented interface stack models for an end station ..... | 149 |
| Figure 23-6 | Two further interface stack modeling choices .....                     | 149 |
| Figure 23-7 | An interface stack model for link aggregation and MACsec.....          | 150 |
| Figure 23-8 | An interface stack with LLDP instances.....                            | 150 |

Tables

Table 19-1 MAC Privacy protection EtherType allocation ..... 86

Table 22-1 Use of ifGeneralInformationGroup Objects ..... 118

Table 22-2 Use of ifCounterDiscontinuityGroup Object..... 119

# IEEE Standard for Local and Metropolitan Area Networks — Media Access Control (MAC) Security Amendment 4: MAC Privacy Protection

[This amendment is based on IEEE Std 802.1AE™-2018.]

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 italics***. 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 ***underline*** (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 1.1 as follows:*

**IEEE 802®** Local Area Networks (LANs) are often deployed in networks that support mission-critical applications. These include corporate networks of considerable extent, and public networks that support many customers with different economic interests. The protocols that configure, manage, and regulate access to these networks typically run over the networks themselves. Preventing disruption and data loss arising from transmission and reception by unauthorized parties is highly desirable, since it is not practical to secure the entire network against physical access by determined attackers.

[The MAC Security protocol](#) (MACsec), as defined by this standard, allows authorized systems that attach to and interconnect LANs in a network to maintain confidentiality of transmitted data and to take measures against frames transmitted or modified by unauthorized devices.

MACsec facilitates

- a) Maintenance of correct network connectivity and services
- b) Isolation of denial of service attacks
- c) Localization of any source of network communication to the LAN of origin
- d) The construction of public networks, offering service to unrelated or possibly mutually suspicious customers, using shared LAN infrastructures
- e) Secure communication between organizations, using a LAN for transmission
- f) Incremental and non-disruptive deployment, protecting the most vulnerable network components

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™ provides authentication and cryptographic key distribution.<sup>1</sup>

MACsec protects communication between trusted components of the network infrastructure, thus protecting the network operation. MACsec cannot protect against attacks facilitated by the trusted components themselves, and is complementary to, rather than a replacement for, end-to-end application-to-application security protocols. The latter can secure application data independent of network operation, but cannot necessarily defend the operation of network components, or prevent attacks using unauthorized communication from reaching the systems that operate the applications.

[MAC Privacy protection protocol, as defined by this standard, can be used in conjunction with MACsec to reduce the ability of adversaries to correlate the MAC addresses, sizes, and transmission timing of user data frames with individual persons, network applications, details of those applications, and levels of application activity.](#)

<sup>1</sup> Information on other references can be found in Clause 2.

## 1.2 Scope

### *Change 1.2 as follows:*

The scope of this standard is to specify provision of connectionless user data confidentiality, frame data integrity, and data origin authenticity by media access independent protocols and entities that operate transparently to MAC Clients.

NOTE—The MAC Clients are as specified in IEEE Std 802, IEEE Std 802.1Q™, and IEEE Std 802.1X™.<sup>2</sup>

To this end it

- a) Specifies the requirements to be satisfied by equipment claiming conformance to this standard.
- b) Specifies the requirements for [MAC Security](#) ~~MACsec~~ in terms of provision of the MAC Service and the preservation of the semantics and parameters of service requests and indications.
- c) Describes the threats, both intentional and accidental, to correct provision of the service.
- d) Specifies security services that prevent, or restrict, the effect of attacks that exploit these threats.
- e) Examines the potential impact of both the threats and the use of MACsec on the Quality of Service (QoS), specifying constraints on the design and operation of MAC Security entities and protocols.
- f) Models support of the secure MAC Service in terms of the operation of media access control method independent MAC Security Entities (SecYs) within the MAC Sublayer.
- g) Specifies the format of the MACsec Protocol Data Unit (MPDUs) used to provide secure service.
- h) Identifies the functions to be performed by each SecY, and provides an architectural model of its internal operation in terms of Processes and Entities that provide those functions.
- i) Specifies each SecY's use of an associated and collocated Port Access Entity (PAE, IEEE Std 802.1X) to discover and authenticate MACsec protocol peers, and its use of that PAE's Key Agreement Entity (KaY) to agree and update cryptographic keys.
- j) Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a SecY.
- k) Specifies how SecYs are incorporated within the architecture of end stations, bridges, and two-port Ethernet Data Encryption devices (EDEs).
- l) Establishes the requirements for management of MAC Security, identifying the managed objects and defining the management operations for SecYs.
- m) Specifies ~~the a~~ Management Information Base (MIB) module for [SecY management](#) ~~managing the operation of MAC Security in TCP/IP networks~~.
- n) [Specifies a YANG configuration and operational state model for SecY management.](#)
- o) Specifies requirements, criteria, and choices of Cipher Suites for use with this standard.
- p) [Describes threats to individual privacy that can result from an adversary's observation of individual frames, even if those frames are integrity protected and their data confidentiality protected.](#)
- q) [Models support of a privacy protected secure MAC Service in terms of the operation of MAC Privacy protection Entities \(PrYs\) that encapsulate user data frames in MAC Privacy protection Protocol Data Units \(MPPDUs\) to hide the user source and destination MAC addresses and to reduce any correlation of the sizes and transmission timing of frames with user identities and communication purposes, applications, or content.](#)
- r) [Specifies the addressing, encoding, and decoding of MPPDUs.](#)
- s) [Identifies the functions to be performed by each PrY, and provides an architectural model of its internal operation in terms of Processes and Entities that provide those functions.](#)

<sup>2</sup> Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

- t) [Specifies performance requirements and recommends default values and applicable ranges for the operational parameters of a PrY.](#)
- u) [Specifies how PrYs can be incorporated within the architecture of end stations, bridges, two-port Ethernet Data Encryption devices \(EDEs\), and bridged networks.](#)
- v) [Describes the requirements for management of MAC Privacy protection, identifying the managed objects and defining the managed objects for PrYs.](#)
- w) [Specifies a Management Information Base \(MIB\) module for PrY management.](#)
- x) [Specifies a YANG configuration and operational state model for PrY management.](#)

## 2. Normative references

*Change the list of normative references in Clause 2 as follows:*

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 802<sup>®</sup>, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.<sup>3,4</sup>

IEEE Std 802.1Q<sup>™</sup>, IEEE Standard for Local and Metropolitan Area Networks: Bridges and Bridged Networks.

IEEE Std 802.1X<sup>™</sup>, IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control.

~~IEEE Std 802.1Xbx<sup>™</sup> 2014, IEEE Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control—Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions.~~

IEEE Std 802.1AB<sup>™</sup>, IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity and Discovery.

IEEE Std 802.1AC<sup>™</sup>, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

IEEE Std 802.3<sup>™</sup>, IEEE Standard for Ethernet.

IETF RFC 1213: Management Information Base for Network Management of TCP/IP-based internets: MIB-II, McCloghrie, K., and Rose, M. T., March 1991.<sup>5</sup>

IETF RFC 2578, STD 58, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and Waldbusser, S., April 1999.

IETF RFC 2579, STD 58, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and Waldbusser, S., April 1999.

IETF RFC 2580, STD 58, Conformance Statements for SMIPv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., and Waldbusser, S., April 1999.

IETF RFC 2863, The Interfaces Group MIB using SMIPv2, McCloghrie, K., and Kastenholz, F., June 2000.

IETF RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), Preshun, R., editor, December 2002.

[IETF RFC 7317, A YANG Data Model for System Management, Bierman, A., Bjorklund, M., August 2014.](#)

[IETF RFC 7950, The YANG 1.1 Data Modeling Language, Bjorklund, M., August 2016.](#)

<sup>3</sup> IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://www.standards.ieee.org>).

<sup>4</sup> The IEEE standards or products referred to in this clause are trademarks of The Institute of Electrical and Electronics Engineers, Inc.

<sup>5</sup> IETF RFCs are available from the Internet Engineering Task Force (<https://www.ietf.org/rfc.html>).

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

[IETF RFC 8343, A YANG Data Model for Interface Management, Bjorklund, M., March 2018.](#)

ISO/IEC 14882, Information Technology—Programming languages—C++.<sup>6</sup>

NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.<sup>7</sup>

---

<sup>6</sup> ISO/IEC documents are available from the International Organization of Standardization (<https://www.iso.org/>) and from the International Electrotechnical Commission (<http://www.iec.ch>). These documents are also available from the American National Standards Institute (<https://www.ansi.org/>).

<sup>7</sup> NIST Special Publications are available from the National Institute of Standards and Technology (<https://csrc.nist.gov/>).

### 3. Definitions

*Change the following definitions in Clause 3 as shown:*

**access priority:** The priority that a client of the MAC Service or MAC Internal Sublayer Service (ISS) associates ~~associated~~ with a given transmit request ~~made by a MAC Security Entity (SecY) at its Common Port~~.

**NOTE—**In this standard a MAC Security Entity (SecY) is a shim that can be a client of a service access point supported (at its lower interface) by a specific media access method, e.g., IEEE Std 802.3, and can provide (at its upper interface) a service access point that is used by its own client. From the point of view of the SecY, the priority associated with each transmit request received from its client is the user priority for that request and the priority associated with the corresponding transmit request that it makes of the underlying service is the access priority.

**Customer Network Port (CNP):** A port on the network component of an Ethernet Data Encryption device (EDE-CS, EDE-CC, or EDE-SS) that provides internal connectivity to the edge component of that EDE.

**Provider Network Port (PNP):** The black-side port of an Ethernet Data Encryption device (EDE-CS, EDE-CC, or EDE-SS).

**user priority:** The priority associated with a transmit request accepted by an entity that provides the MAC Service or MAC Internal Sublayer Service (ISS) ~~received by the Controlled Port of a MAC Security Entity (SecY)~~.

*Insert the following terms and definitions in Clause 3 in alphabetical order:*

**express frame:** A frame that a protocol entity identifies as a candidate for early transmission using **preemption** capabilities.

**NOTE—**Not all protocol entities that forward a given frame need identify that frame as an express frame or a preemptable frame. In this standard that identification uses the priority of the frame.

**preemptable frame:** A frame that a protocol entity identifies as a candidate for suspension by **preemption** capabilities, so as to allow the earlier transmission of an **express frame**.

**preemption:** The temporary suspension of the transmission (or encoding for transmission) of a **preemptable frame** to allow the earlier transmission of an **express frame**.

**NOTE—**The preemption capabilities specified by IEEE Std 802.3 can be used in conjunction with the MAC Security protocol (MACsec) to expedite the transmission of an **express frame** that becomes available for transmission after transmission of a **preemptable frame** has begun. The MAC Privacy protection protocol also supports preemption, allowing the encoding of an express frame prior to the encoding of the remaining fragment(s) of a preemptable frame.

**Privacy Channel:** A sequence of frames with the same MAC source and destination addresses each conveying a single MAC Privacy Protocol Data Unit (MPPDU), with the sequence conveying a sequence of entire or fragmented user data frames and padding.

**NOTE—**In this standard all unqualified references to “fragments” and “fragmentation” are to MPPDU encoding.

**Privacy Frame:** A frame that conveys a single MAC Privacy Protocol Data Unit (MPPDU) that includes a single, unfragmented, user data frame followed by zero or more octets of padding.

**Private Port:** The access point used to provide the privacy protected secure MAC Service to a client of a MAC Privacy protection Entity (PrY).

**shim:** A protocol entity that uses the same service as it provides.

**NOTE—**Shims specified or referenced in this standard secure the ISS, enhance privacy, or provided multiplexing over separate instances of the ISS.

**traffic:** A sequence of frames forwarded in a network.

## 4. Abbreviations and acronyms

*Insert the following abbreviations and acronyms in Clause 4 in alphabetical order:*

|        |                                                      |
|--------|------------------------------------------------------|
| ATS    | Asynchronous Traffic Shaping                         |
| C-TAG  | C-VLAN tag                                           |
| C-VID  | Customer VLAN Identifier                             |
| C-VLAN | Customer Virtual Local Area Network                  |
| CNP    | Customer Network Port                                |
| MPP    | MAC Privacy protection <sup>8</sup>                  |
| MPPDU  | MAC Privacy protection Protocol Data Unit            |
| MPPCI  | MAC Privacy protection Protocol Component Identifier |
| PBN    | Provider Bridged Network                             |
| PCI    | Personal Correlatable Information                    |
| PII    | Personally Identifiable Information                  |
| PNP    | Provider Network Port                                |
| PrY    | MAC Privacy protection Entity                        |
| PSFP   | Per-Stream Filtering and Policing                    |
| PVID   | port VLAN Identifier                                 |
| S-VLAN | Service Virtual Local Area Network                   |
| TPMR   | Two-Port MAC Relay                                   |
| VID    | VLAN Identifier                                      |
| VLAN   | Virtual Local Area Network                           |
| YANG   | Yet Another Next Generation <sup>9</sup>             |

<sup>8</sup> The acronym MPP is used in figures.

<sup>9</sup> YANG is best viewed as a name, not an acronym.

## 5. Conformance

*Change the introductory text of Clause 5 as follows:*

A claim of conformance to this standard [for the implementation of MAC Security](#) is a claim that the behavior of an implementation of a MAC Security Entity (SecY) meets the requirements of this standard [\(5.3, 5.4\)](#) 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 [for the implementation of MAC Security](#) 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 ~~a~~ 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.

Conformance to this standard does not require any restriction as to the nature of the system of which a SecY forms part other than as constrained by the SecY's required and optional capabilities (5.3, 5.4). Clause 11 describes the use of SecYs within a number of different types of systems. These include, but are not limited to, systems specified in IEEE Std 802.1Q and those that make use of IEEE Std 802.1X. Successful interoperable use of MACsec in those systems also requires conformance to those standards. In addition Clause 15 of this standard makes use of components specified in IEEE Std 802.1Q to define further systems, Ethernet Data Encryption devices (EDEs), whose purpose is to secure the MAC Service within networks comprising bridging systems specified by IEEE Std 802.1Q in a way that is transparent to the operation of those bridging systems. Additional claims of conformance can be made to this standard in respect of EDEs (5.5–5.7).

[A claim of conformance to this standard for the implementation of MAC Privacy protection is a claim that the behavior of an implementation of a MAC Privacy protection entity \(PrY\) meets the requirements of this standard \(5.10, 5.11\) as they apply to the operation of the MAC Privacy protection protocol, management of its operation, and provision of service to the protocol clients of the PrY, as revealed through externally observable behavior of the system of which the PrY forms a part.](#)

[Conformance to this standard does not require any restriction as to the nature of the system of which a PrY forms part other than as constrained by the PrY's required and optional capabilities. Clause 21 describes the deployment of PrYs in a number of different types of system and network scenarios.](#)

*This amendment does not make changes to 5.1 Requirements terminology, but includes it to provide clarity in requirements terminology at all stages of review, and in the use of the published amendment prior to its inclusion in a revision of the base standard:*

### 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 proformas (see Annex A.5.2) reflect 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*.

*Change 5.2 as follows:*

## 5.2 Protocol Implementation Conformance Statements (PICS)

The supplier of a MAC Security Entity (SecY) 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.

The supplier of an EDE that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex D (normative) and shall provide the information necessary to identify both the supplier and the implementation. The supplier of an EDE implementation shall also complete or provide copies of the following PICS proforma(s) adhering to any restrictions required by conformance to this standard and marking any exceptions required by conformance to this standard:

- a) For all types of EDE, the PICS proforma for each SecY implementation provided in Annex A of this standard.
- b) For all types of EDE, the PICS proforma specified by IEEE Std 802.1X.
- c) For an EDE-M: the IEEE Std 802.1Q PICS proforma as required for a VLAN-unaware MAC Bridge.
- d) For an EDE-CS: the IEEE Std 802.1Q PICS proforma as required for a Provider Edge Bridge.
- e) For an EDE-CC: the IEEE Std 802.1Q PICS proforma as required for each of the two C-VLAN components.
- f) For an EDE-SS: the IEEE Std 802.1Q PICS proforma as required for each of the two S-VLAN components.

The supplier of a MAC Privacy protection Entity (PrY) implementation that is claimed to conform to this standard shall complete a copy of the PICS proforma provided in Annex H (normative) and shall provide the information necessary to identify both the supplier and the implementation.

## 5.5 EDE Conformance

*Change the third paragraph and following text of 5.5 as follows:*

An implementation of any type of EDE that is claimed to conform to this standard shall

- a) Have two and only two externally accessible Bridge Ports, a red-side port and a black-side port.  
NOTE—A red-side port can also be referred to as the *customer* or *edge* port and the black-side port as a *provider* or *network* port. The use of either or both of the pair of terms, *customer/provider* and *edge/network* to refer to an EDE-M's ports is consistent with the relative roles played by ports in multicomponent bridges and EDEs.
- b) Associate a Port Access Entity (PAE) that includes a MACsec Key Agreement Entity (KaY) capable of operating MKA with each SecY required by this standard for the particular type of EDE (15.2, 15.4, 15.5, 15.6, 15.7).

[An implementation of any type of EDE that is claimed to conform to this standard may](#)

- c) [Provide MAC Privacy protection for black-side port interface stack clients with a MAC Privacy protection entity \(PrY\) that uses the secure MAC Service provided by that port's SecY \(21.5\).](#)

*Change 5.8 as follows:*

## 5.8 EDE-CC conformance

An implementation of an EDE-CC (15.6) that is claimed to conform to this standard shall

- a) Comprise two C-VLAN [bridge](#) components, each as specified by IEEE Std 802.1Q—~~(5.5 of IEEE Std 802.1Q-2018)~~—an edge component and a network component—internally connected as specified in 15.6.
- b) Incorporate a SecY in each of the internal Provider Edge Port interface stacks (15.6).
- c) Be capable of being configured to use the EDE-CC PAE group address as the destination MAC address of group addressed EAPOL PDUs for group addressed EAPOL PDUs (as specified in 15.6).
- d) Filter and not forward all frames whose destination MAC address is either one of the addresses identified by IEEE Std 802.1Q as a C-VLAN component Reserved Address or the EDE-CC PAE group address.

[An EDE-CC that is not capable of providing MAC Privacy protection shall](#)

- e) Transmit frames received from the red-side customer port and relayed to the black-side network port untagged if they were received untagged and C-tagged with the same C-VID if they were C-tagged on receipt (15.6).

[An EDE-CC that is capable of providing MAC Privacy protection \[5.5c\)\] shall](#)

- f) [Be capable of being configured to transmit frames received from the red-side customer port and relayed to the black-side network port untagged if they were received untagged and C-tagged with the same C-VID if they were C-tagged on receipt \(15.6\).](#)

[An EDE-CC that is capable of providing MAC Privacy protection \[5.5c\)\] may](#)

- g) [Be capable, when relaying a frame received on the red-side customer port, of using the received C-VID to select the C-VID to be used when tagging the MACsec protected frame for transmission by the black-side network port \(15.6\).](#)

*NOTE—This optional capability was added by the IEEE Std 802.1AE-2023 MAC Privacy protection amendment to this standard to hide the use of two or more customer VLANs for traffic destined for the same peer PrY. Its use requires additional management and care in deployment. The frame transmitted through a peer red-side port, after protected transmission over a service provider network, is that originally received by the EDE.*

*Insert the following text (subclauses 5.10 and 5.11) after subclause 5.9:*

## 5.10 MAC Privacy protection Entity requirements

An implementation of a MAC Privacy protection Entity (PrY) for which conformance to this standard is claimed shall

- a) Support the Private and Controlled Ports as specified in Clause 20.
- b) Support the MAC status and point-to-point parameters for the Private Port as specified in 20.4.
- c) Transmit only MPPDUs whose encoding satisfies the constraints specified in 19.6.
- d) Support requests to transmit user data frames through the Private Port as specified in 20.5 through 20.10.

- e) Support per priority privacy selection (unprotected, as an individual Privacy Frame, or in a Privacy Channel) of user data frames transmitted by the client of the PrY's Private Port, as specified in 20.5.
- f) Support unprotected user data frame transmission, with the ability to manage the access priority used to transmit that frame, as specified in 20.6.
- g) Support individual Privacy Frame transmission, with the ability to manage the access priority used to transmit that frame, as specified in 20.7.
- h) Support the configuration of two, one, or no transmit Privacy Channels as specified in 20.8.
- i) Support the generation of Privacy Channel MPPDUs as specified in 20.9.
- j) Be capable of being configured to use the default Privacy Channel MPPDU generation algorithm specified in 20.9.4.
- k) Accept user data frames for Privacy Channel encapsulation as specified in 20.10.
- l) Be capable of being configured to use the default Privacy Channel MPPDU encapsulation algorithm specified in 20.10.1.
- m) Transmit all MPPDUs using the same destination MAC Address and the same source MAC Address as specified in 18.1.
- n) Use the PAE Group Address that is being used by MKA as the destination MAC Address of transmitted MPPDUs and to recognize received MPPDUs when the PrY's Controlled Port is directly supported by a SecY (17.4, 18.1, 21.1.1).
- o) Use the MAC Address used to generate MACsec SCI(s) as the source MAC Address of transmitted MPPDUs when the PrY's Controlled Port is directly supported by a SecY, as specified in 18.1.
- p) Support administrative configuration of the destination MAC Address used to transmit MPPDUs if and when the PrY's Controlled Port is not directly supported by a SecY as an individual or group MAC address (18.1, 20.14).
- q) Use a MAC Address associated with the PrY's interface stack as the source MAC Address of transmitted MPPDUs if and when the PrY is not directly supported by a SecY, as specified in 18.1.
- r) Recognize received MPPDUs as specified in 20.11.
- s) Validate and extract received MPPDU components as specified in 20.12 and 19.7.
- t) Support simultaneous reassembly of Express and Preemptable frames from received Frame Fragments as specified in 20.13.
- u) Deliver user data frames received in Encapsulated Frame components and reassembled from received Frame Fragments in the order specified in 20.13.
- v) Be capable of being configured to use the default reassembly algorithm as specified in 20.13.1 to simultaneously reassemble Express Frame Fragments and Preemptable Frame Fragments transmitted by a single peer.

## 5.11 MAC Privacy protection Entity options

An implementation of a MAC Privacy protection Entity (PrY) for which conformance to this standard is claimed may

- a) Be capable of being configured to use the default reassembly algorithm as specified in 20.13.1. for reception from a specified number (greater than one) of peer PrYs, each transmitting Express Frame Fragments and Preemptable Frame Fragments.
- b) Use Private Port transmit request stream\_handles to select Privacy Selection Table entries (20.5.2).

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

### 10.7 SecY management

*Insert the following text after the second paragraph of 10.7:*

Figure 10-5 includes data made available, through the LMI, to a SecY by other components (notably the KaY) within the same system, and data and operations that a SecY makes available to those components, in addition to operations and parameters accessible by one or more remote management protocols. Security considerations, and the utility of transient data, restrict management access to some parameters and operations. For particular managed object specifications based on this clause and figure, see Clause 13 (MAC Security Entity MIB) and Clause 23 (YANG Data Models).

*Insert the following NOTE after NOTE 1 in 10.7, and renumber the NOTE that follows.*

NOTE 2—Figure 10-5 was revised by IEEE Std 802.1AE-2022 to provide cross-references and to indicate the accessibility, read (r) or write (w) status of parameters that can be managed by remote management protocol, as specified for the SecY MIB module (Clause 13) or the YANG module (Clause 23). Whether access to particular management parameters is permitted is also subject to security considerations, as described for each of those modules.

*Change the third paragraph of 10.7 as follows:*

In Figure 10-5 the management information for each SecY is shown as indexed by controlledPortNumber within a SecY System. This containment relationship complements that specified in IEEE Std 802.1X, where the management information for each PAE is indexed by portNumber (12.9.2 of IEEE Std 802.1X-2010) within a PAE System and includes the controlledPortNumber that identifies the Controlled Port of the associated SecY. The containment relationship also matches that specified in Clause 13 (MAC Security Entity MIB) and Clause 23 (YANG Data Models). In the MIB module a , -with-a-SecY System corresponds ing to a SecY MIB module instance, and each controlledPortNumber to the ifIndex (IETF RFC 2863) value used to identify a SecY within that module (13.3.2, 13.5). In the YANG module the management information for each PrY is indexed by an interfaceName.

*Insert the following paragraph prior to the paragraph in 10.7 beginning “Conformance to this standard is strictly ...”*

The representation of the time of the occurrence of an event, such as the creation time for a receive SC (see 10.7.12, 10.7.14, 10.7.21, 10.7.23, 10.7.28), can depend on the management protocol used to convey that information. In SNMP sysUpTime, the time for which the SNMP agent has been running, is used. In YANG the wall-clock date-and-time is used.

*Delete the last paragraph of 10.7, beginning “In some situations it can be desirable to substitute control using SNMP for the operation of key agreement protocols ...”*

*Replace Figure 10-5 with the following figure:*



28

### 10.7.3 Uncontrolled Port statistics

*Insert the following NOTE after the last paragraph of 10.7.3:*

NOTE—The names of 32-bit counters specified by IETF RFC 2863 have been used to identify statistics, avoiding the need for a mapping from this standard's terminology to that specified for the Interfaces Group MIB. The use of 64-bit counters can be required to support that MIB, as specified in 3.1.6 of IETF RFC 2863, with the lower 32-bits reported when object is accessed using the names specified in a), b), e), and f) above. The corresponding 64-bit counter names are ifHCInOctets, ifHCInUcastPkts, ifHCInMulticastPkts, ifHCInBroadcastPkts, ifHCIOctets, ifHCOUcastPkts, ifHCOMulticastPkts, and ifHCOBroadcastPkts. Corresponding 64-bit YANG data nodes are specified by IETF RFC 8343.

### 10.7.6 Controlled Port statistics

*Insert the following NOTES after the last paragraph of 10.7.6:*

NOTE 1—The names of 32-bit counters specified by IETF RFC 2863 have been used to identify statistics, avoiding the need for a mapping from this standard's terminology to that specified for the Interfaces Group MIB. The use of 64-bit counters can be required to support that MIB, as specified in 3.1.6 of IETF RFC 2863, with the lower 32-bits reported when object is accessed using the names specified in a), b), e), and f) above. The corresponding 64-bit counter names are ifHCInOctets, ifHCInUcastPkts, ifHCInMulticastPkts, ifHCInBroadcastPkts, ifHCIOctets, ifHCOUcastPkts, ifHCOMulticastPkts, and ifHCOBroadcastPkts. Corresponding 64-bit YANG data nodes are specified by IETF RFC 8343.

NOTE 2—Separate per SecY 64-bit counters for InPktsNoTAG, InPktsOverrun, InPktsBadTag, and InPktsNoSA, and separate per SC 64-bit counters for InPktsLate, and inPktsNotValid, are required to support the MIB and YANG modules specified in this standard (10.7.9, 13.6, Clause 23).

## 13. MAC Security Entity MIB

### 13.1 Introduction

*Insert a NOTE after the text of 13.1 as follows:*

NOTE—Annex G (informative) provides a detailed history and rationale for changes to SecY management and this MIB module. Normative changes to compliance and conformance statements are also described in 13.5.

#### 13.3.2 Relationship to the Interfaces MIB

*Replace Figure 13-1 with the following:*

|                                               |                                                 |
|-----------------------------------------------|-------------------------------------------------|
| Controlled Port<br>Interface<br>(ifEntry = k) | Uncontrolled Port<br>Interface<br>(ifEntry = j) |
| Physical Interface<br>(ifEntry = i)           |                                                 |

**Figure 13-1—MACsec Interface Stack**

## 13.6 MAC Security Entity (SecY) MIB definition<sup>10, 11</sup>

*Replace the text of 13.6 with the following:*

```
IEEE8021-SECY-MIB DEFINITIONS ::= BEGIN

-- =====
-- IEEE802.1AE MAC Security Entity (SecY) MIB
-- =====

IMPORTS
    MODULE-IDENTITY, OBJECT-TYPE,
    Unsigned32, Integer32, Counter32, Counter64
        FROM SNMPv2-SMI
    TEXTUAL-CONVENTION, RowPointer, TimeStamp, TruthValue, RowStatus
        FROM SNMPv2-TC
    SnmpAdminString
        FROM SNMP-FRAMEWORK-MIB
    MODULE-COMPLIANCE, OBJECT-GROUP
        FROM SNMPv2-CONF
    InterfaceIndex, ifCounterDiscontinuityGroup
        FROM IF-MIB
    ;

ieee8021SecyMIB MODULE-IDENTITY
    LAST-UPDATED "202206060000Z" -- June 6, 2022
    ORGANIZATION "IEEE 802.1 Working Group"
    CONTACT-INFO
        " WG-URL: http://www.ieee802.org/1/
          WG-EMail: stds-802-1-l@ieee.org
          Contact: IEEE 802.1 Working Group Chair
          Postal: C/O IEEE 802.1 Working Group
                  IEEE Standards Association
                  445 Hoes Lane
                  Piscataway, NJ 08854
                  USA
          E-mail: stds-802-1-chairs@ieee.org"
    DESCRIPTION
        "The MAC security entity (SecY) MIB module. A SecY is a shim in an interface
        stack that uses the MAC Security (MACsec) protocol.

        Copyright (C) IEEE (2021).
        This version of this MIB module is part of IEEE Std 802.1AE-2022;
        see that standard for full legal notices.

        Unless otherwise indicated, the references in this MIB module are to
        IEEE Std 802.1AE-2018 as amended by IEEE Std 802.1AE-2018/Cor 1-2020 and
        IEEE Std 802.1AE-2022.

        Each SecY transmits MACsec protected frames on one or more
        Secure Channels (SCs) to each of the other SecYs attached to the
        same LAN and participating in the same Secure Connectivity
        Association (CA). The CA is a security relationship, that is
        established and maintained by key agreement protocols and supported
        by MACsec to provide full connectivity between its participants.
        Each SC provides unidirectional point to multipoint connectivity
        from one participant to all the others and is supported by a
        succession of similarly point to multipoint Secure Associations
        (SAs). The Secure Association Key (SAK) used to protect frames is
        changed as an SA is replaced by its (overlapping) successor so
        fresh keys can be used without disrupting a long lived SC and CA.

        Two different upper interfaces, a Controlled Port (for frames
```

<sup>10</sup> Copyright release for MIBs: Users of this standard may freely reproduce the MIB modules in this standard so that they can be used for their intended purpose.

<sup>11</sup> The MIB text in this clause includes clickable cross-references to MIB objects ([highlighted](#)). A plain text (UTF-8) version of this MIB is attached to the PDF version of this standard, and can be obtained by Web browser from the IEEE 802.1 Website at <https://1.ieee802.org/mib-modules/>.

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

protected by MACsec, providing an instance of the secure MAC service) and an Uncontrolled Port (for frames not requiring protection, like the key agreement frames used to establish the CA and distribute keys) are associated with a SecY shim. For each instance of a SecY two ifTable rows (one for each interface) run on top of an ifTable row representing the 'Common Port' interface, such as a row with ifType = 'ethernetCsmacd(6)'.

|                                                                                 |                                                                                     |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| Controlled Port Interface<br>(ifEntry = j, ifType =<br>macSecControlledIF(231)) | Uncontrolled Port Interface<br>(ifEntry = k, ifType =<br>macSecUncontrolledIF(232)) |
| Physical Interface<br>(ifEntry = i)<br>(ifType = ethernetCsmacd(6))             |                                                                                     |

Example MACsec Interface Stack. i, j, k are ifIndexes each indicating a row in the ifTable.

"

REVISION "202206060000Z" -- June 6, 2022  
DESCRIPTION

"Published as part of IEEE Std 802.1AE-2022.  
Cross references, contact information, and descriptions updated."

REVISION "201712071816Z"  
DESCRIPTION

"Published as part of IEEE Std 802.1AE-2018.  
Updated CONTACT-INFO."

REVISION "201605102049Z"  
DESCRIPTION

"Updated by the IEEE Std 802.1AEcg amendment. Object DESCRIPTIONS and references aligned with text of the standard (including prior amendments). IEEE 802.1AEcg Annex G details changes. The initial version of this ieee8021SecyMIB used the object name prefix 'secy' rather than 'ieee8021secy' (recommended by RFC 4181). The 'secy' prefix has been retained in this revision for backwards compatibility and internal consistency."

REVISION "200601100000Z"  
DESCRIPTION "Initial version of this MIB in IEEE 802.1AE-2006"  
::= { iso(1) std(0) iso8802(8802) ieee802dot1(1)  
ieee802dot1mibs(1) 3 }

-- =====  
-- Textual Conventions

SecySCI ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"Textual convention for a Secure Channel Identifier (SCI).

Each SC is identified by an SCI comprising a 48-bit MAC Address, allocated to the transmitting system and a 16-bit Port Identifier."

REFERENCE "7.1.2, Figure 7-7"

SYNTAX OCTET STRING (SIZE (8))

SecyAN ::= TEXTUAL-CONVENTION

DISPLAY-HINT "d"

STATUS current

DESCRIPTION

"Textual convention for an Association Number (AN).

Each SC is comprised of a succession of SAs, each with a different SAK, identified by a Secure Association Identifier (SAI) comprising an SCI concatenated with a two-bit AN. The SAI is unique for SAs used by SecYs participating in a given CA at any instant."

REFERENCE "7.1.3, Figure 7-7"

SYNTAX Unsigned32 (0..3)

-- =====  
-- subtrees in the SecY MIB

```

secyMIBNotifications      OBJECT IDENTIFIER ::= { ieee8021SecyMIB 0 }
secyMIBObjects            OBJECT IDENTIFIER ::= { ieee8021SecyMIB 1 }
    secyMgmtMIBObjects    OBJECT IDENTIFIER ::= { secyMIBObjects 1 }
    secyStatsMIBObjects   OBJECT IDENTIFIER ::= { secyMIBObjects 2 }
secyMIBConformance        OBJECT IDENTIFIER ::= { ieee8021SecyMIB 2 }
    secyMIBCompliances    OBJECT IDENTIFIER ::= { secyMIBConformance 1 }
    secyMIBGroups         OBJECT IDENTIFIER ::= { secyMIBConformance 2 }
=====
--secyMgmtMIBObjects
-- secyIfTable
-- secyTSCTable --
-- secyTSATable --
-- secyIfTCTable --
-- secyIfAPTable --
-- secyRxSCTable
-- secyRxSATable
-- secyCipherSuiteTable
-- secyIfCipherTable
--The following are historic following approval of IEEE Std 802.1AEcg-2017,
--even if their STATUS remains 'current'. They do not include any objects
--that are part of a current conformance OBJECT-GROUP, and lack traffic
--class transmit SC and XPN support:
-- secyTxSCTable, secyTxSATable
-- =====
-- secyIfTable
secyIfTable      OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyIfEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table with an entry for each MAC Security protocol (MACsec) capable
        interface in the system, i.e. for each SecY. Configured value of writable
        objects in each table entry MUST be persistent and remain unchanged across
        re-initialization of the system's management entity."
    REFERENCE   "10.7, Table 13-1"
    ::= { secyMgmtMIBObjects 1 }

--secyIfEntry
secyIfEntry      OBJECT-TYPE
    SYNTAX      SecyIfEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "A table entry with service information for a particular SecY."
    INDEX       { secyIfInterfaceIndex }
    ::= { secyIfTable 1 }

--SecyIfEntry
SecyIfEntry ::= SEQUENCE {
    secyIfInterfaceIndex      InterfaceIndex,
    secyIfMaxPeerSCs          Unsigned32,
    secyIfRxMaxKeys           Unsigned32,
    secyIfTxMaxKeys           Unsigned32,
    secyIfProtectFramesEnable TruthValue,
    secyIfValidateFrames      INTEGER,
    secyIfReplayProtectEnable TruthValue,
    secyIfReplayProtectWindow Unsigned32,
    secyIfCurrentCipherSuite  Unsigned32,
    secyIfAdminPt2PtMAC       INTEGER,
    secyIfOperPt2PtMAC        TruthValue,
    secyIfIncludeSCIEnable    TruthValue,
    secyIfUseESEnable         TruthValue,
    secyIfUseSCBEnable        TruthValue,
    secyIfSCI                 SecySCI,
    secyIfIncludingSCI         TruthValue,
    secyIfMaxTSCs             Unsigned32
}

```

```
--secyIfInterfaceIndex
secyIfInterfaceIndex    OBJECT-TYPE
    SYNTAX      InterfaceIndex
    MAX-ACCESS   not-accessible
    STATUS      current
    DESCRIPTION  "The Interface Index for this SecY's Controlled Port."
    REFERENCE   "10.1"
    ::= { secyIfEntry 1 }

--secyIfMaxPeerSCs
secyIfMaxPeerSCs        OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "security connections"
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION  "The maximum number of peer SCs for this SecY."
    REFERENCE   "10.7.7"
    ::= { secyIfEntry 2 }

--secyIfRxMaxKeys
secyIfRxMaxKeys          OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "keys"
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION  "The maximum number of keys in simultaneous use for
    reception for this SecY."
    REFERENCE   "10.7.7"
    ::= { secyIfEntry 3 }

--secyIfTxMaxKeys
secyIfTxMaxKeys          OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "keys"
    MAX-ACCESS   read-only
    STATUS      current
    DESCRIPTION  "The maximum number of keys in simultaneous use for
    transmission for this SecY."
    REFERENCE   "10.7.16"
    ::= { secyIfEntry 4 }

--secyIfProtectFramesEnable
secyIfProtectFramesEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS   read-write
    STATUS      current
    DESCRIPTION  "Enables or disables protection of transmitted frames."
    REFERENCE   "10.7.17, Figure 10-3"
    DEFVAL { true }
    ::= { secyIfEntry 5 }

--secyIfValidateFrames
secyIfValidateFrames      OBJECT-TYPE
    SYNTAX      INTEGER {
        disabled(1),
        check(2),
        strict(3),
        null(4)    -- 802.1AEcg
    }
    MAX-ACCESS   read-write
    STATUS      current
    DESCRIPTION  "Controls validation of received frames.
    disabled(1) : disable validation, remove SecTAGs and ICVs (if present.
    check(2)    : enable validation, do not discard invalid frames.
    strict(3)   : enable validation and discard invalid frames.
    null(4)     : no processing, do not remove SecTAGs or ICVs."
    REFERENCE   "10.7.8, Figure 10-4"
    DEFVAL { strict }
    ::= { secyIfEntry 6 }
```

```
--secyIfReplayProtectEnable
secyIfReplayProtectEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION  "Enables or disables replay protection."
    REFERENCE   "10.7.8, Figure 10-4"
    DEFVAL { true }
    ::= { secyIfEntry 7 }

--secyIfReplayProtectWindow
secyIfReplayProtectWindow OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "Packets"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION  "The replay protection window size."
    REFERENCE   "10.7.8, Figure 10-4"
    DEFVAL { 0 }
    ::= { secyIfEntry 8 }

--secyIfCurrentCipherSuite
secyIfCurrentCipherSuite OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION  "The secyCipherSuiteTableindex for this SecY's in use Cipher
                  Suite. Should be read-only if secyIfCipherTable implemented."
    REFERENCE   "10.7.25"
    ::= { secyIfEntry 9 }

--secyIfAdminPt2PtMAC
secyIfAdminPt2PtMAC OBJECT-TYPE
    SYNTAX      INTEGER {
        forceTrue(1),
        forceFalse(2),
        auto(3)
    }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION  "Controls the value of operPointToPointMAC (secyOperPt2PtMAC)
                  reported to the user(s) of this SecY's Controlled Port:

    forceTrue(1) : operPointToPointMAC is True, regardless of the
                    configuration and status of the SecY.
    forceFalse(2) : operPointToPointMAC is False, regardless of the
                    configuration and status of the SecY.
    auto(3)      : OperPointMAC is True if secyIfvalidateFrames is
                    strict and reception is from at most one peer SecY,
                    or if secyIfvalidateFrames is not strict and
                    operPointToPointMAC is True for the Common Port,
                    and is False otherwise."
    REFERENCE   "6.5, 10.7.4"
    DEFVAL { auto }
    ::= { secyIfEntry 10 }

--secyIfOperPt2PtMAC
secyIfOperPt2PtMAC OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "Reflects the current service connectivity to be assumed by the
                  user(s) of the SecY's Controlled Port:

    true(1) : connectivity is to at most one other system.
    false(2) : connectivity is to one or more other systems."
    REFERENCE   "6.5, 10.7.4"
    ::= { secyIfEntry 11 }
```

```
--secyIfIncludeSCIEnable
secyIfIncludeSCIEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION  "Mandates inclusion of an explicit SCI in the SecTAG
                  when transmitting protected frames."
    REFERENCE   "10.5.3 alwaysIncludeSCI, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 12 }

--secyIfUseESEnable
secyIfUseESEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION  "Enables use of the ES bit in the SecTAG when
                  transmitting protected frames."
    REFERENCE   "10.5.3 useES, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 13 }

--secyIfUseSCBEnable
secyIfUseSCBEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION  "Enables use of the SCB bit in the SecTAG when
                  transmitting protected frames."
    REFERENCE   "10.5.3 useSCB, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 14 }

--secyIfSCI
secyIfSCI OBJECT-TYPE
    SYNTAX      SecySCI
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The SCI for the SecY's default traffic class."
    REFERENCE   "7.1.2, 10.7.1"
    ::= { secyIfEntry 15 }

--secyIfIncludingSCI
secyIfIncludingSCI OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "True if an explicit SCI is included in the SecTAG when
                  transmitting protected frames."
    REFERENCE   "10.5.3 includingSCI, 10.7.17"
    DEFVAL { false }
    ::= { secyIfEntry 16 }

--secyIfMaxTSCs
secyIfMaxTSCs OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "security connections"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The maximum number of transmit SCs for this SecY."
    REFERENCE   "10.7.16"
    ::= { secyIfEntry 17 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
-- =====
--secyTSCTable
secyTSCTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTSCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "A transmit SC management table for systems with SecY's capable
                  of supporting traffic class SCs."
    REFERENCE   "7.1.2, 10.7.17, 10.7.20"
    ::= { secyMgmtMIBObjects 10 }

--secyTSCEntry
secyTSCEntry OBJECT-TYPE
    SYNTAX      SecyTSCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "An entry with transmit SC information for one of the system's
                  SecYs and one of its traffic classes."
    INDEX { secyIfInterfaceIndex, secyTSCI }
    ::= { secyTSCTable 1 }

--SecyTSCEntry
SecyTSCEntry ::= SEQUENCE {
    secyTSCI          SecySCI,
    secyTSCState      INTEGER,
    secyTSCEncodingSA RowPointer,
    secyTSCCreatedTime TimeStamp,
    secyTSCStartedTime TimeStamp,
    secyTSCStoppedTime TimeStamp
}

--secyTSCI
secyTSCI OBJECT-TYPE
    SYNTAX      SecySCI
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "The SCI for the transmit SC for this SecY and traffic class."
    REFERENCE   "7.1.2, 10.7.17, 10.7.20"
    ::= { secyTSCEntry 1 }

--secyTSCState
secyTSCState OBJECT-TYPE
    SYNTAX      INTEGER { inUse(1), notInUse(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The state of the transmit SC for this SecY and traffic class:
                  inUse(1) : one or more SAs are in use.
                  notInUse(2) : no SAs are in use for this SC."
    REFERENCE   "10.7.20"
    ::= { secyTSCEntry 2 }

--secyTSCEncodingSA
secyTSCEncodingSA OBJECT-TYPE
    SYNTAX      RowPointer
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The SA currently used to encode the SecTAG. The row pointer points to an
                  entry in the secyTSATable. If no such information is available, the value
                  shall be the OBJECT IDENTIFIER { 0 0 }."
    REFERENCE   "10.5.1, 10.7.21"
    ::= { secyTSCEntry 3 }

--secyTSCCreatedTime
secyTSCCreatedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The system time when this transmitting SC was created."
    REFERENCE   "10.7.21"
    ::= { secyTSCEntry 4 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyTSCStartedTime
secyTSCStartedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this SC last started transmitting."
    REFERENCE   "10.7.21"
    ::= { secyTSCEntry 5 }

--secyTSCStoppedTime
secyTSCStoppedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this SC last stopped transmitting."
    REFERENCE   "10.7.21"
    ::= { secyTSCEntry 6 }

-- =====
--secyTSATable
secyTSATable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A transmit SA management table for systems with SecY's capable
                of supporting traffic class SC's."
    REFERENCE   "10.7.22, Table 13-2"
    ::= { secyMgmtMIBObjects 11 }

--secyTSAEntry
secyTSAEntry OBJECT-TYPE
    SYNTAX      SecyTSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry for a transmit SA."
    INDEX       { secyIfInterfaceIndex, secyTSCI, secyTSA }
    ::= { secyTSATable 1 }

--SecyTSAEntry
SecyTSAEntry ::= SEQUENCE {
    secyTSA                SecyAN,
    secyTSASState          INTEGER,
    secyTSANextXPN         Counter64,
    secyTSAConfidentiality TruthValue,
    secyTSAKeyIdentifier   SnmpAdminString,
    secyTSASSCI            Integer32,
    secyTSACreatedTime     TimeStamp,
    secyTSAStartedTime     TimeStamp,
    secyTSAStoppedTime     TimeStamp
}

--secyTSA
secyTSA OBJECT-TYPE
    SYNTAX      SecyAN
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "The association number (AN) for this transmit SA."
    REFERENCE   "10.7.22"
    ::= { secyTSAEntry 1 }

--secyTSASState
secyTSASState OBJECT-TYPE
    SYNTAX      INTEGER { inUse(1), notInUse(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The transmit SA current status: inUse(1) , notInUse(2).".
    REFERENCE   "10.7.23"
    ::= { secyTSAEntry 2 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyTSANextXPN
secyTSANextXPN OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The next packet number (PN) for this SA."
    REFERENCE   "10.5, 10.7.23"
    ::= { secyTSAEntry 3 }

--secyTSAConfidentiality
secyTSAConfidentiality OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if the SA provides confidentiality."
    REFERENCE   "10.7.23"
    ::= { secyTSAEntry 4 }

--secyTSAKeyIdentifier
secyTSAKeyIdentifier OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (1..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The Key Identifier (KI) for the SAK for this SA."
    REFERENCE   "IEEE 802.1X, 10.7.23"
    ::= { secyTSAEntry 5 }

--secyTSASSCI
secyTSASSCI OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The SSCI for this SA, 0 if not using an XPN Cipher Suite."
    REFERENCE   "IEEE 802.1X, 10.7.23"
    ::= { secyTSAEntry 6 }

--secyTSACreatedTime
secyTSACreatedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this transmit SA was created."
    REFERENCE   "10.7.23"
    ::= { secyTSAEntry 7 }

--secyTSASTartedTime
secyTSASTartedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this SA last started transmitting."
    REFERENCE   "10.7.23"
    ::= { secyTSAEntry 8 }

--secyTSASToppedTime
secyTSASToppedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this SA last stopped transmitting."
    REFERENCE   "10.7.23"
    ::= { secyTSAEntry 9 }
```

```
-- =====
--secyRxSCTable
secyRxSCTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyRxSCEnter
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "A table of receive SCs for the system."
    REFERENCE   "10.7.11, Table 13-2"
    ::= { secyMgmtMIBObjects 4 }

--secyRxSCEnter
secyRxSCEnter OBJECT-TYPE
    SYNTAX      SecyRxSCEnter
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "A table entry for a receive SC."
    INDEX       { secyIfInterfaceIndex, secyRxSCI }
    ::= { secyRxSCTable 1 }

--SecyRxSCEnter
SecyRxSCEnter ::= SEQUENCE {
    secyRxSCI          SecySCI,
    secyRxSCState      INTEGER,
    secyRxSCCurrentSA  RowPointer, -- deprecated
    secyRxSCCreatedTime Timestamp,
    secyRxSCStartedTime Timestamp,
    secyRxSCStoppedTime Timestamp
}

--secyRxSCI
secyRxSCI OBJECT-TYPE
    SYNTAX      SecySCI
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "The SCI for the receive SC."
    REFERENCE   "10.7.11"
    ::= { secyRxSCEnter 1 }

--secyRxSCState
secyRxSCState OBJECT-TYPE
    SYNTAX      INTEGER {inUse(1), notInUse(2)}
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The receive SCs current state:
        inUse(1) : one or more SAs for this SC are in use.
        notInUse(2) : no SAs for this SC is in use."
    REFERENCE   "10.7.12 receiving, 10.7.14 inUse, 10.7.15"
    ::= { secyRxSCEnter 2 }

--secyRxSCCurrentSA
secyRxSCCurrentSA OBJECT-TYPE
    SYNTAX      RowPointer
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION  "The current receiving association number for the SC in use.
        The row pointer points to an entry in the secyRxSatable. If no
        such information can be identified, the value of this object shall
        be the OBJECT IDENTIFIER { 0 0 }."
    REFERENCE   "10.7.15, 10.7.13"
    ::= { secyRxSCEnter 3 }

--secyRxSCCreatedTime
secyRxSCCreatedTime OBJECT-TYPE
    SYNTAX      Timestamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The system time when this receiving SC was created."
    REFERENCE   "10.7.12"
    ::= { secyRxSCEnter 4 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyRxSCStartedTime
secyRxSCStartedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this SC last started receiving."
    REFERENCE   "10.7.12"
    ::= { secyRxSCEntry 5 }

--secyRxSCStoppedTime
secyRxSCStoppedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The system time when this SC last stopped receiving."
    REFERENCE   "10.7.12"
    ::= { secyRxSCEntry 6 }

-- =====
--secyRxSatable
secyRxSatable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyRxSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table with entries for the system's receive SAs."
    REFERENCE   "10.7.13"
    ::= { secyMgmtMIBObjects 5 }

--secyRxSAEntry
secyRxSAEntry OBJECT-TYPE
    SYNTAX      SecyRxSAEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry for one of the SAs used by one of the system's
                SecY's to receive protected frames."
    INDEX       { secyIfInterfaceIndex, secyRxSCI, secyRxSA }
    ::= { secyRxSatable 1 }

--SecyRxSAEntry
SecyRxSAEntry ::= SEQUENCE {
    secyRxSA          SecyAN,
    secyRxSAState     INTEGER,
    secyRxSASNextPN   Unsigned32,      -- deprecated
    secyRxSASAKUnchanged TruthValue,   -- deprecated
    secyRxSACreatedTime TimeStamp,
    secyRxSASStartedTime TimeStamp,
    secyRxSASStoppedTime TimeStamp,
    secyRxSASNextXPN  Counter64,
    secyRxSASLowestXPN Counter64,
    secyRxSAKeyIdentifier SnmpAdminString,
    secyRxSASSCI      Integer32
}

--secyRxSA
secyRxSA OBJECT-TYPE
    SYNTAX      SecyAN
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "This receive SA's association number (AN)."
    REFERENCE   "10.7.13"
    ::= { secyRxSAEntry 1 }

--secyRxSAState
secyRxSAState OBJECT-TYPE
    SYNTAX      INTEGER { inUse(1), notInUse(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "This receive SA's current state."
    REFERENCE   "10.7.14"
    ::= { secyRxSAEntry 2 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyRxSANextPN
secyRxSANextPN OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS   read-write
    STATUS       deprecated
    DESCRIPTION  "Use secyRxSANextXPN for both 32-bit PN and 64-bit XPN values.
                  If implemented, this object contains the lower 32 bits."
    REFERENCE   "10.6.5, 10.7.14, Figure 10-4"
    ::= { secyRxSAEntry 3 }

--secyRxSASAKUnchanged
secyRxSASAKUnchanged OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS   read-only
    STATUS       deprecated -- 802.1AEcg
    DESCRIPTION  "An SAK reference, unchanged for the receiving SA's life."
    REFERENCE   "10.7.13"
    ::= { secyRxSAEntry 4 }

--secyRxSACreatedTime
secyRxSACreatedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "The system time when this receiving SA was created."
    REFERENCE   "10.7.14"
    ::= { secyRxSAEntry 5 }

--secyRxSASStartedTime
secyRxSASStartedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "The system time when this SA last started receiving."
    REFERENCE   "10.7.14"
    ::= { secyRxSAEntry 6 }

--secyRxSASStoppedTime
secyRxSASStoppedTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "The system time when this SA last stopped receiving frames."
    REFERENCE   "10.7.14"
    ::= { secyRxSAEntry 7 }

--secyRxSANextXPN
secyRxSANextXPN OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "One more than the highest PN conveyed in the SecTAG of
                  successfully validates frames received on this SA."
    REFERENCE   "10.6.5, 10.7.14, Figure 10-4"
    ::= { secyRxSAEntry 8 }

--secyRxSALowestXPN
secyRxSALowestXPN OBJECT-TYPE
    SYNTAX      Counter64
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION  "The lowest acceptable packet number. A received frame
                  with a lower PN is discarded if
                  secyIfReplayProtectEnable is enabled."
    REFERENCE   "10.6.2, 10.6.4, 10.6.5, 10.7.14,
                  Figure 10-4"
    ::= { secyRxSAEntry 9 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AEdk-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyRxSAKeyIdentifier
secyRxSAKeyIdentifier OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (1..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The Key Identifier (KI) for the SAK for this SA."
    REFERENCE   "IEEE 802.1X, 10.7.14"
    ::= { secyRxSAEntry 10 }

--secyRxSASSCI
secyRxSASSCI OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION  "The SSCI for this SA, 0 if an XPN Cipher Suite is not in use."
    REFERENCE   "IEEE 802.1X, 10.7.14"
    ::= { secyRxSAEntry 11 }

-- =====
--secyCipherSuiteTable
secyCipherSuiteTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyCipherSuiteEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "A table of the system's Cipher Suite capabilities, which can differ
    with the same secyCipherSuiteId. The secyIfCipherTable lists
    available entries by SecY, avoiding the need for remote network
    management to write objects or create rows in this table. Any
    configured values shall be stored in persistent memory and remain
    unchanged across a re-initialization of the management system."
    REFERENCE   "10.7.25"
    ::= { secyMgmtMIBObjects 6 }

--secyCipherSuiteEntry
secyCipherSuiteEntry OBJECT-TYPE
    SYNTAX      SecyCipherSuiteEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "An entry for a Cipher Suite implementation."
    INDEX { secyCipherSuiteIndex }
    ::= { secyCipherSuiteTable 1 }

--SecyCipherSuiteEntry
SecyCipherSuiteEntry ::= SEQUENCE {
    secyCipherSuiteIndex      Unsigned32,
    secyCipherSuiteId         OCTET STRING,
    secyCipherSuiteName       SnmpAdminString,
    secyCipherSuiteCapability BITS,
    secyCipherSuiteProtection BITS,
    secyCipherSuiteProtectionOffset INTEGER,
    secyCipherSuiteDataLengthChange TruthValue,
    secyCipherSuiteICVLength  Unsigned32,
    secyCipherSuiteRowStatus  RowStatus
}

--secyCipherSuiteIndex
secyCipherSuiteIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION  "The CipherSuiteTable entry index."
    ::= { secyCipherSuiteEntry 1 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyCipherSuiteId
secyCipherSuiteId OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (8))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION  "A unique 64-bit (EUI-64) identifier for the Cipher
                  Suite."
    REFERENCE   "10.7.25, Table 14-1"
    ::= { secyCipherSuiteEntry 2 }

--secyCipherSuiteName
secyCipherSuiteName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (1..128))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION  "The Cipher Suite Name, 128 octets or fewer."
    REFERENCE   "10.7.25, Table 14-1"
    ::= { secyCipherSuiteEntry 3 }

--secyCipherSuiteCapability
secyCipherSuiteCapability OBJECT-TYPE
    SYNTAX      BITS {
                    integrity(0),
                    confidentiality(1),
                    offsetConfidentiality(2)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION  "Cipher Suite implementation capability information.

                    integrity(0)           : integrity protection.
                    confidentiality(1)      : confidentiality protection.
                    offsetConfidentiality(2) : offset confidentiality
                    protection."
    REFERENCE   "10.7.24, 10.7.25"
    ::= { secyCipherSuiteEntry 4 }

--secyCipherSuiteProtection
secyCipherSuiteProtection OBJECT-TYPE
    SYNTAX      BITS {
                    integrity(0),
                    confidentiality(1),
                    offsetConfidentiality(2)
                }
    MAX-ACCESS  read-create
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION  "The secyIfCipherSuite table supports per SecY configuration and should be
                  used instead of this object. If the secyCipherSuiteCapability integrity
                  bit is on, it can be turned on for this object. If the integrity and
                  confidentiality bits of the secyCipherSuiteCapability are both on, the
                  confidentiality bit of this object can be turned on provided that the
                  integrity bit is also turned on, and the offsetConfidentiality bit can
                  also be turned on if the secyCipherSuiteCapability has that bit on.

                  integrity(0)           : enable (on) or disable integrity protection.
                  confidentiality(1)      : enable (on) or disable confidentiality protection.
                  offsetConfidentiality(2) : enable (on) or disable offset confidentiality."
    REFERENCE   "10.7.25"
    DEFVAL { { integrity } }
    ::= { secyCipherSuiteEntry 5 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyCipherSuiteProtectionOffset
secyCipherSuiteProtectionOffset OBJECT-TYPE
    SYNTAX      Integer32 (0 | 30 | 50)
    UNITS        "bytes"
    MAX-ACCESS   read-create
    STATUS        deprecated -- 802.1AEcg
    DESCRIPTION
        "The confidentiality protection offset options provided by the cipher
        suite. Can only be non-zero if the secyCipherSuiteProtection offset
        confidentiality bit is on, and then can only be 0 if the confidentiality
        bit is on."
    REFERENCE    "10.7.25, 10.7.26"
    DEFVAL { 0 }
    ::= { secyCipherSuiteEntry 6 }

--secyCipherSuiteDataLengthChange
secyCipherSuiteDataLengthChange OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS   read-create
    STATUS        current
    DESCRIPTION  "True if cipher suite changes the length of the data."
    REFERENCE    "10.7.25, Figure 9-1"
    ::= { secyCipherSuiteEntry 7 }

--secyCipherSuiteICVLength
secyCipherSuiteICVLength OBJECT-TYPE
    SYNTAX      Unsigned32 (8..16)
    UNITS        "octets"
    MAX-ACCESS   read-create
    STATUS        current
    DESCRIPTION  "The length of the integrity check value (ICV) field."
    REFERENCE    "10.7.25, Figure 9-1"
    ::= { secyCipherSuiteEntry 8 }

--secyCipherSuiteRowStatus
secyCipherSuiteRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS   read-create
    STATUS        current
    DESCRIPTION
        "The secyIfCipherTable (if implemented) avoids the need for
        network manager creation of entries in the secyCipherSuiteTable,
        and RowStatus should always be valid(1), with any per SecY
        unavailability indicated by an absence of a corresponding
        secyIfCipherTable entry or one with secyCipherSuiteAvailable
        false (the latter can indicate temporary unavailability)."
    REFERENCE    "10.7.25"
    ::= { secyCipherSuiteEntry 9 }

-- =====
--secyIfCipherTable
secyIfCipherTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyIfCipherEntry
    MAX-ACCESS   not-accessible
    STATUS        current
    DESCRIPTION
        "A table with an entry for the Cipher Suite capabilities
        implemented for each SecY in this system, providing per SecY
        control of Cipher Suite use.

        The configured value of writable objects in each table entry
        shall be stored in persistent memory and remain unchanged across
        a re-initialization of the system's management entity."
    REFERENCE    "10.7.26, Table 13-1"
    ::= { secyMgmtMIBObjects 7 }
```

```
--secyIfCipherEntry
secyIfCipherEntry OBJECT-TYPE
    SYNTAX      SecyIfCipherEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table entry with Cipher Suite control for a SecY."
    INDEX       { secyIfInterfaceIndex, secyCipherSuiteIndex }
    ::= { secyIfCipherTable 1 }

--SecyIfCipherEntry
SecyIfCipherEntry ::= SEQUENCE {
    secyIfCipherImplemented TruthValue,
    secyIfCipherEnableUse   TruthValue,
    secyIfCipherRqConfidentiality TruthValue
}

--secyIfCipherImplemented
secyIfCipherImplemented OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "True if the Cipher Suite implementation can be used by
                this SecY (if secyIfCipherEnableUse is true)."
    REFERENCE   "10.7.26"
    DEFVAL { true }
    ::= { secyIfCipherEntry 1 }

--secyIfCipherEnableUse
secyIfCipherEnableUse OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "Enables use of the Cipher Suite by this SecY."
    REFERENCE   "10.7.26"
    DEFVAL { true }
    ::= { secyIfCipherEntry 2 }

--secyIfCipherRqConfidentiality
secyIfCipherRqConfidentiality OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "True if confidentiality protection (without an offset)
                is required if this Cipher Suite is used."
    REFERENCE   "10.7.26"
    DEFVAL { true }
    ::= { secyIfCipherEntry 3 }

-- =====
--secyIfTCTable
secyIfTCTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyIfTCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The Traffic Class Table for each SecY in this system.
        The configured value of writable objects in each table entry
        MUST be stored in persistent memory and remain unchanged across
        a re-initialization of the system's management entity."
    REFERENCE   "10.5.1, 10.7.17, Table 13-1"
    ::= { secyMgmtMIBObjects 8 }

--secyIfTCEntry
secyIfTCEntry OBJECT-TYPE
    SYNTAX      SecyIfTCEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table entry providing Traffic Class selection for a given
                SecY and user priority."
    INDEX       { secyIfInterfaceIndex, secyIfTCUserPriority }
    ::= { secyIfTCTable 1 }
```

```
--SecyIfTCEntry
SecyIfTCEntry ::= SEQUENCE {
    secyIfTCUserPriority      Integer32,
    secyIfTCTrafficClass     Integer32
}

--secyIfTCUserPriority
secyIfTCUserPriority OBJECT-TYPE
    SYNTAX      Integer32 (0..7)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "One of the possible user priority values for a frame."
    REFERENCE   "10.7.17"
    ::= { secyIfTCEntry 1 }

--secyIfTCTrafficClass
secyIfTCTrafficClass OBJECT-TYPE
    SYNTAX      Integer32 (0..7)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "The Traffic Class for this SecY and user priority, as
        transmitted in the four most significant bits of the Port
        Identifier component of the SCI of protected frames."
    REFERENCE   "10.7.17"
    DEFVAL { 0 }
    ::= { secyIfTCEntry 2 }

-- =====
--secyIfAPTable
secyIfAPTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyIfAPEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "The Access Priority Table for each SecY in this system.
        The configured value of writable objects in each table entry
        MUST be stored in persistent memory and remain unchanged across
        a re-initialization of the system's management entity."
    REFERENCE   "10.5.1, 10.7.17, Table 13-1"
    ::= { secyMgmtMIBObjects 9 }

--secyIfAPEntry
secyIfAPEntry OBJECT-TYPE
    SYNTAX      SecyIfAPEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table entry for a given SecY, selecting the access priority
        and the drop_eligible parameter value used for a given user
        priority and drop_eligible parameter value."
    INDEX { secyIfInterfaceIndex, secyIfAPUserPCP }
    ::= { secyIfAPTable 1 }

--SecyIfAPEntry
SecyIfAPEntry ::= SEQUENCE {
    secyIfAPUserPCP      Integer32,
    secyIfAPAccessPCP    Integer32
}

--secyIfAPUserPCP
secyIfAPUserPCP OBJECT-TYPE
    SYNTAX      Integer32 (0..15)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "The user priority (3 more significant bits) and drop_eligible
        parameter (least significant bit) values."
    REFERENCE   "10.5, 10.7.17"
    ::= { secyIfAPEntry 1 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyIfAPAccessPCP
secyIfAPAccessPCP OBJECT-TYPE
    SYNTAX      Integer32 (0..15)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION "The access priority (3 more significant bits) and drop_eligible
                parameter (least significant bit) values."
    REFERENCE   "10.5, 10.7.17"
    ::= { secyIfAPEntry 2 }

--
=====
--secyTxSCTable
secyTxSCTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSCEnter
    MAX-ACCESS  not-accessible
    STATUS      current -- ??
    DESCRIPTION "A transmit SC management table for systems not supporting
                traffic class SC's, with an entry for each SecY."
    REFERENCE   "10.7.17, 10.7.20, Table 13-2"
    ::= { secyMgmtMIBObjects 2 }

--secyTxSCEnter
secyTxSCEnter OBJECT-TYPE
    SYNTAX      SecyTxSCEnter
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "An entry with transmit SC information for a SecY."
    INDEX { secyIfInterfaceIndex }
    ::= { secyTxSCTable 1 }

--SecyTxSCEnter
SecyTxSCEnter ::= SEQUENCE {
    secyTxSCI          SecySCI,
    secyTxSCState      INTEGER,
    secyTxSCEncodingSA RowPointer,
    secyTxSCEncipheringSA RowPointer, -- deprecated
    secyTxSCCreatedTime TimeStamp,
    secyTxSCStartedTime TimeStamp,
    secyTxSCStoppedTime TimeStamp
}

--secyTxSCI
secyTxSCI OBJECT-TYPE
    SYNTAX      SecySCI
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The SCI for the SecY's transmit SC."
    REFERENCE   "7.1.2, 10.7.1"
    ::= { secyTxSCEnter 1 }

--secyTxSCState
secyTxSCState OBJECT-TYPE
    SYNTAX      INTEGER { inUse(1), notInUse(2) }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The transmitting state of the SecY's transmit SC."
    REFERENCE   "10.7.21 transmitting, 10.7.23"
    ::= { secyTxSCEnter 2 }

--secyTxSCEncodingSA
secyTxSCEncodingSA OBJECT-TYPE
    SYNTAX      RowPointer
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The SA currently used to encode the SecTAG for frames awaiting transmission.
                The row pointer points to an entry in the secyTxSatable. If no such
                information is available, the value shall be the OBJECT IDENTIFIER { 0 0 }."
    REFERENCE   "10.5.1, 10.7.21"
    ::= { secyTxSCEnter 3 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyTxSCEncipheringSA
secyTxSCEncipheringSA    OBJECT-TYPE
    SYNTAX      RowPointer
    MAX-ACCESS    read-only
    STATUS      deprecated
    DESCRIPTION
        "The SA currently used to encipher frames for transmission.
         The row pointer points to an entry in the secyTxSatable. If no such
         information is available, the value shall be the OBJECT IDENTIFIER { 0 0 }."
    REFERENCE    "10.5.4"
    ::= { secyTxSCEntry 4 }

--secyTxSCCreatedTime
secyTxSCCreatedTime      OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS    read-only
    STATUS      current
    DESCRIPTION  "The system time when this transmitting SC was created."
    REFERENCE    "10.7.21"
    ::= { secyTxSCEntry 5 }

--secyTxSCStartedTime
secyTxSCStartedTime      OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS    read-only
    STATUS      current
    DESCRIPTION  "The system time when this SC last started transmitting."
    REFERENCE    "10.7.21"
    ::= { secyTxSCEntry 6 }

--secyTxSCStoppedTime
secyTxSCStoppedTime      OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS    read-only
    STATUS      current
    DESCRIPTION  "The system time when this SC last stopped transmitting."
    REFERENCE    "10.7.21"
    ::= { secyTxSCEntry 7 }

-- =====
--secyTxSatable
secyTxSatable            OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyTxSAEntry
    MAX-ACCESS    not-accessible
    STATUS      current
    DESCRIPTION  "A transmit SA management table for a system with no SecYs
                 capable of supporting traffic class transmit SCs."
    REFERENCE    "10.7.22, Table 13-2"
    ::= { secyMgmtMIBObjects 3 }

--secyTxSAEntry
secyTxSAEntry            OBJECT-TYPE
    SYNTAX      SecyTxSAEntry
    MAX-ACCESS    not-accessible
    STATUS      current
    DESCRIPTION  "An entry for a transmit SA."
    INDEX       { secyIfInterfaceIndex, secyTxSA }
    ::= { secyTxSatable 1 }

--SecyTxSAEntry
SecyTxSAEntry ::= SEQUENCE {
    secyTxSA                SecyAN,
    secyTxSAState            INTEGER,
    secyTxSANextPN           Unsigned32,
    secyTxSAConfidentiality  TruthValue,
    secyTxSASAKUnchanged     TruthValue, -- deprecated
    secyTxSACreatedTime      TimeStamp,
    secyTxSAStartedTime      TimeStamp,
    secyTxSASToppedTime      TimeStamp
}
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyTxSA
secyTxSA          OBJECT-TYPE
    SYNTAX         SecyAN
    MAX-ACCESS     not-accessible
    STATUS         current
    DESCRIPTION    "The association number (AN) for this transmit SA."
    REFERENCE      "10.7.22"
    ::= { secyTxSAEntry 1 }

--secyTxSAState
secyTxSAState     OBJECT-TYPE
    SYNTAX         INTEGER {inUse(1), notInUse(2)}
    MAX-ACCESS     read-only
    STATUS         current
    DESCRIPTION    "The transmit SAs current status: inUse(1), notInUse(2)."
```

```
    REFERENCE      "10.7.22"
    ::= { secyTxSAEntry 2 }

--secyTxSANextPN
secyTxSANextPN    OBJECT-TYPE
    SYNTAX         Unsigned32
    MAX-ACCESS     read-only
    STATUS         current
    DESCRIPTION    "The next packet number (PN) for this SA."
    REFERENCE      "10.5, 10.7.23"
    ::= { secyTxSAEntry 3 }

--secyTxSAConfidentiality
secyTxSAConfidentiality OBJECT-TYPE
    SYNTAX         TruthValue
    MAX-ACCESS     read-only
    STATUS         current
    DESCRIPTION    "True if the SA provides confidentiality as well as
                    integrity for transmitted frames."
    REFERENCE      "10.7.23"
    ::= { secyTxSAEntry 4 }

--secyTxSASAKUnchanged
secyTxSASAKUnchanged OBJECT-TYPE
    SYNTAX         TruthValue
    MAX-ACCESS     read-only
    STATUS         deprecated
    DESCRIPTION    "A reference to an SAK that is unchanged for the life
                    of the transmitting SA."
    REFERENCE      "10.7.22"
    ::= { secyTxSAEntry 5 }

--secyTxSACreatedTime
secyTxSACreatedTime OBJECT-TYPE
    SYNTAX         TimeStamp
    MAX-ACCESS     read-only
    STATUS         current
    DESCRIPTION    "The system time when this transmit SA was created."
    REFERENCE      "10.7.23"
    ::= { secyTxSAEntry 6 }

--secyTxSASStartedTime
secyTxSASStartedTime OBJECT-TYPE
    SYNTAX         TimeStamp
    MAX-ACCESS     read-only
    STATUS         current
    DESCRIPTION    "The system time when this SA last started transmitting."
    REFERENCE      "10.7.23"
    ::= { secyTxSAEntry 7 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyTxSASStoppedTime
secyTxSASStoppedTime          OBJECT-TYPE
    SYNTAX          TimeStamp
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION     "The system time when this SA last stopped transmitting."
    REFERENCE       "10.7.23"
    ::= { secyTxSAEntry 8 }

-- =====
--secyStatsMIBObjects
-- secyTSCStatsTable
-- secyRxSCStatsTable
-- secyRxSASStatsTable
-- secyStatsTable
--The following are historic following approval of IEEE Std 802.1AEcg-2017,
--even if their STATUS remains 'current'. They do not include any objects
--that are part of a current conformance OBJECT-GROUP, and lack traffic
--class transmit SC and XPN support:
-- secyTxSCStatsTable, secyTxSASStatsTable
-- =====
--secyTSCStatsTable
secyTSCStatsTable          OBJECT-TYPE
    SYNTAX          SEQUENCE OF SecyTSCStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION     "A table of statistics for each SecY's transmit SCs."
    REFERENCE       "10.7.18, 10.7.19, Figure 10-3"
    ::= { secyStatsMIBObjects 12 }

--secyTSCStatsEntry
secyTSCStatsEntry          OBJECT-TYPE
    SYNTAX          SecyTSCStatsEntry
    MAX-ACCESS      not-accessible
    STATUS          current
    DESCRIPTION     "A entry containing counts for a transmit SC, since SA counters
                    are reset when the SA's AN is reused these are a summation for
                    all current and prior SAs belonging to the SC."
    AUGMENTS { secyTSCEntry }
    ::= { secyTSCStatsTable 1 }

--SecyTSCStatsEntry
SecyTSCStatsEntry ::= SEQUENCE {
    secyTSCStatsProtectedPkts Counter64,
    secyTSCStatsEncryptedPkts Counter64
}

--secyTSCStatsProtectedPkts
secyTSCStatsProtectedPkts  OBJECT-TYPE
    SYNTAX          Counter64
    UNITS           "Packets"
    MAX-ACCESS      read-only
    STATUS          current
    DESCRIPTION     "The number of integrity protected but not encrypted packets
                    for this transmit SC."
    REFERENCE       "10.7.18, Figure 10-3"
    ::= { secyTSCStatsEntry 1 }
```

```
--secyTSCStatsEncryptedPkts
secyTSCStatsEncryptedPkts OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "The number of integrity protected and encrypted packets for
         this transmit SC."
    REFERENCE   "10.7.18, Figure 10-3"
    ::= { secyTSCStatsEntry 2 }

-- =====
--secyRxSASStatsTable
secyRxSASStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyRxSASStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      deprecated
    DESCRIPTION
        "A table that contains the statistics objects for each
         receiving SA in the MAC security entity."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyStatsMIBObjects 3 }

--secyRxSASStatsEntry
secyRxSASStatsEntry OBJECT-TYPE
    SYNTAX      SecyRxSASStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION
        "An entry with statistics for a receive SA. The AN that
         identifies an SA (for a given SC) and this corresponding entry
         can be reused. When creating the SA and before (re)using the
         entry, the SA counters are (re)set to 0. When the SA is stopped
         (secyRxSA notInuse) the counters stop incrementing.

         The secyRxSASStatsTable timestamps SA creation, start, and stop."
    AUGMENTS { secyRxSAEntry }
    ::= { secyRxSASStatsTable 1 }

--SecyRxSASStatsEntry
SecyRxSASStatsEntry ::= SEQUENCE {
    secyRxSASStatsUnusedSAPkts Counter32, -- deprecated
    secyRxSASStatsNoUsingSAPkts Counter32, -- deprecated
    secyRxSASStatsNotValidPkts Counter32, -- deprecated
    secyRxSASStatsInvalidPkts Counter32, -- deprecated
    secyRxSASStatsOKPkts Counter32 -- deprecated
}

--secyRxSASStatsUnusedSAPkts
secyRxSASStatsUnusedSAPkts OBJECT-TYPE
    SYNTAX      Counter32
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
        "For this SA which is not currently in use, the number of
         received, unencrypted, packets with secyValidateFrames
         not in the strict mode."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSASStatsEntry 1 }
```

```
--secyRxSASStatsNoUsingSAPkts
secyRxSASStatsNoUsingSAPkts OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "Packets"
    MAX-ACCESS   read-only
    STATUS        deprecated
    DESCRIPTION
        "For this SA which is not currently in use, the number of
        received packets that have been discarded, and have
        either the packets encrypted or secyValidateFrames set to
        strict mode."
    REFERENCE    "10.7.9, Figure 10-4"
    ::= { secyRxSASStatsEntry 4 }

--secyRxSASStatsNotValidPkts
secyRxSASStatsNotValidPkts OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "Packets"
    MAX-ACCESS   read-only
    STATUS        deprecated
    DESCRIPTION
        "For this SA, the number discarded packets with the
        condition that the packets are not valid and one of the
        following conditions are true: either secyValidateFrames in
        strict mode or the packets encrypted."
    REFERENCE    "10.7.9, Figure 10-4"
    ::= { secyRxSASStatsEntry 13 }

--secyRxSASStatsInvalidPkts
secyRxSASStatsInvalidPkts OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "Packets"
    MAX-ACCESS   read-only
    STATUS        deprecated
    DESCRIPTION
        "For this SA, the number of packets with the condition
        that the packets are not valid and secyValidateFrames is in
        check mode."
    REFERENCE    "10.7.9, Figure 10-4"
    ::= { secyRxSASStatsEntry 16 }

--secyRxSASStatsOKPkts
secyRxSASStatsOKPkts OBJECT-TYPE
    SYNTAX      Counter32
    UNITS        "Packets"
    MAX-ACCESS   read-only
    STATUS        deprecated
    DESCRIPTION
        "For this SA, the number of validated packets."
    REFERENCE    "10.7.9, Figure 10-4"
    ::= { secyRxSASStatsEntry 25 }

-- =====
--secyRxSCStatsTable
secyRxSCStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyRxSCStatsEntry
    MAX-ACCESS   not-accessible
    STATUS        current
    DESCRIPTION  "A table of statistics for each receive SC for each of
    the system's SecYs."
    REFERENCE    "10.7.9, 10.7.9, Figure 10-4"
    ::= { secyStatsMIBObjects 4 }
```

```
--secyRxSCStatsEntry
secyRxSCStatsEntry OBJECT-TYPE
    SYNTAX      SecyRxSCStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing counts for a receive SC. SA counters are
         reset when the SA's AN is reused, so these SC counts are a
         summation for all current and prior SAs belonging to the SC."
    AUGMENTS { secyRxSCEntEntry }
    ::= { secyRxSCStatsTable 1 }

--SecyRxSCStatsEntry
SecyRxSCStatsEntry ::= SEQUENCE {
    secyRxSCStatsUnusedSAPkts Counter64, -- deprecated
    secyRxSCStatsNoUsingSAPkts Counter64, -- deprecated
    secyRxSCStatsLatePkts Counter64,
    secyRxSCStatsNotValidPkts Counter64,
    secyRxSCStatsInvalidPkts Counter64,
    secyRxSCStatsDelayedPkts Counter64,
    secyRxSCStatsUncheckedPkts Counter64,
    secyRxSCStatsOKPkts Counter64,
    secyRxSCStatsOctetsValidated Counter64, -- deprecated
    secyRxSCStatsOctetsDecrypted Counter64 -- deprecated
}

--secyRxSCStatsUnusedSAPkts
secyRxSCStatsUnusedSAPkts OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The sum of secyRxSASStatsUnusedSAPkts counts for all
                 current and prior SAs belonging to this SC."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 1 }

--secyRxSCStatsNoUsingSAPkts
secyRxSCStatsNoUsingSAPkts OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "The sum of secyRxSASStatsNoUsingSAPkts counts for all
                 current and prior SAs belonging to this SC."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 2 }

--secyRxSCStatsLatePkts
secyRxSCStatsLatePkts OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Count of packets discarded for this SC, with a received PN
                 lower than the lowest acceptable PN (secyRxSALowestXPN) while
                 secyIfReplayProtectEnable was true."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 3 }

--secyRxSCStatsNotValidPkts
secyRxSCStatsNotValidPkts OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Count of packets discarded for this SC, because validation
                 failed and they were encrypted (unrecoverable) or
                 secyIfvalidateFrames was 'strict'."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 4 }
```

# ISO/IEC/IEEE 8802-1AE:2020/Amd.4:2024(en)

IEEE Std 802.1AE-2023  
IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security—Amendment 4: MAC Privacy Protection

```
--secyRxSCStatsInvalidPkts
secyRxSCStatsInvalidPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Count of packets received for this SC, that failed validation
                but were received unencrypted while secyIfvalidateFrames
                was 'check'."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 5 }

--secyRxSCStatsDelayedPkts
secyRxSCStatsDelayedPkts    OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Count of packets received for this SC, with PN lower than
                the lowest acceptable PN (secyRxSALowestXPN) while
                secyIfReplayProtectEnable was false."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 6 }

--secyRxSCStatsUncheckedPkts
secyRxSCStatsUncheckedPkts  OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Count of packets received for this SC while
                secyValidateFrames was 'disabled'."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 7 }

--secyRxSCStatsOKPkts
secyRxSCStatsOKPkts         OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "Count of packets received for this SC that were
                successfully validated and within the replay window."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyRxSCStatsEntry 8 }

--secyRxSCStatsOctetsValidated
secyRxSCStatsOctetsValidated OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Octets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "Count of plaintext octets recovered from packets that were
                integrity protected but not encrypted."
    REFERENCE   "Deprecated, the secyIsStatsTable has per SecY counts
                for cryptographic performance management."
    ::= { secyRxSCStatsEntry 9 }

--secyRxSCStatsOctetsDecrypted
secyRxSCStatsOctetsDecrypted OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Octets"
    MAX-ACCESS  read-only
    STATUS      deprecated -- 802.1AEcg
    DESCRIPTION "Count of plaintext octets recovered from packets
                that were integrity protected and encrypted."
    REFERENCE   "Deprecated, the secyIsStatsTable has per SecY counts
                for cryptographic performance management."
    ::= { secyRxSCStatsEntry 10 }
```

```
-- =====
--secyStatsTable
secyStatsTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF SecyStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION "A table of statistics for each of the system's SecYs."
    REFERENCE   "10.7.9, 10.7.18, Figure 10-3, 10.5"
    ::= { secyStatsMIBObjects 5 }

--secyStatsEntry
secyStatsEntry OBJECT-TYPE
    SYNTAX      SecyStatsEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "An entry containing counts for a SecY."
    AUGMENTS { secyIfEntry }
    ::= { secyStatsTable 1 }

--SecyStatsEntry
SecyStatsEntry ::= SEQUENCE {
    secyStatsTxUntaggedPkts Counter64,
    secyStatsTxTooLongPkts Counter64,
    secyStatsRxUntaggedPkts Counter64,
    secyStatsRxNoTagPkts Counter64,
    secyStatsRxBadTagPkts Counter64,
    secyStatsRxUnknownSCIPkts Counter64, -- deprecated
    secyStatsRxNoSCIPkts Counter64, -- deprecated
    secyStatsRxOverrunPkts Counter64,
    secyStatsRxNoSAPkts Counter64, -- 802.1AECg
    secyStatsRxNoSAErrorPkts Counter64, -- 802.1AECg
    secyStatsTxOctetsProtected Counter64, -- 802.1AECg
    secyStatsTxOctetsEncrypted Counter64, -- 802.1AECg
    secyStatsRxOctetsValidated Counter64, -- 802.1AECg
    secyStatsRxOctetsDecrypted Counter64 -- 802.1AECg
}

--secyStatsTxUntaggedPkts
secyStatsTxUntaggedPkts OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of packets transmitted without a SecTAG
        because secyProtectFramesEnable is configured false."
    REFERENCE   "10.7.18, Figure 10-3"
    ::= { secyStatsEntry 1 }

--secyStatsTxTooLongPkts
secyStatsTxTooLongPkts OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of transmit packets discarded because their
        length is greater than the ifMtu of the Common Port."
    REFERENCE   "10.7.18, Figure 10-3"
    ::= { secyStatsEntry 2 }

--secyStatsRxUntaggedPkts
secyStatsRxUntaggedPkts OBJECT-TYPE
    SYNTAX      Counter64
    UNITS       "Packets"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION "The number of packets without the MACsec tag (SecTAG)
        received while secyValidateFrames was not 'strict'."
    REFERENCE   "10.7.9, Figure 10-4"
    ::= { secyStatsEntry 3 }
```