



Automotive MACsec Specification

MACsec Specification for Automotive Ethernet

Version	1.0
Date	May 16, 2025
Status	Final
Restriction Level	Public

VERSION AND RESTRICTION HISTORY OF THIS DOCUMENT

VERSION	DESCRIPTION	RESTRICTION LEVEL	DATE
1.0	Automotive MACsec specifications	Public	16.05.2025

CHAIR AND VICE CHAIR

CHAIR	NAME	ORGANIZATION
OPEN Alliance TC17 Chair	Oliver Creighton	BMW
OPEN Alliance TC17 Vice Chair	John Moore	Ford Motors
OPEN Alliance TC17 Automotive MACsec subgroup chair	Geet Modi	Texas Instruments

EDITOR

NAME	ORGANIZATION
Geet Modi	Texas Instruments

CONTRIBUTORS

NAME	ORGANIZATION
Giuseppe Tofanicchio	STMicroelectronics International NV
Guillermo Oliver	Analog Devices
Prabhakar Kushwaha	Marvell
Thierry Walrant	NXP
Lars Völker	Technica Engineering GmbH
Kartrin Weiden	BMW
Venkat Arunarthi	Broadcom
Fernando Barbero	KDPOF
Luisma Torres	KDPOF
Haipeng Hu	Volvo Cars
Sundar Ayyasamy	Infineon
Nikita Singh	Texas Instruments
Friedrich Wiemer	Bosch
Hung Yu Lin	Realtek Semiconductor Corporation

Table of Contents

VERSION AND RESTRICTION HISTORY OF THIS DOCUMENT	2
CHAIR AND VICE CHAIR	2
EDITOR	2
CONTRIBUTORS	2
1 OPEN SPECIFICATION OWNERSHIP AND USAGE RIGHTS.....	4
2 RIGHTS AND USAGE RESTRICTIONS SPECIFIC TO OPEN ALLIANCE MEMBERS	4
2.1 Rights and Usage Restrictions Specific to Non-members of OPEN Alliance	5
3 TERMS APPLICABLE TO BOTH MEMBERS AND NON-MEMBERS OF OPEN ALLIANCE..	5
3.1 Patents, Trademarks, and other Rights:	5
3.2 Disclaimers and Limitations of Liability:.....	6
3.3 Compliance with Laws and Regulations:.....	6
3.4 Automotive Applications Only:	7
3.5 Right to Withdraw or Modify:.....	7
4 ABBREVIATION/SYMBOLS	8
5 TERMS AND DEFINITIONS	9
6 NORMATIVE REFERENCES	9
7 INTRODUCTION	10
8 SCOPE	10
9 INTRODUCTION TO AUTOMOTIVE MACSEC – (SPECIFICATIONS)	10
10 CHANGES TO IEEE 802.1AE-2018 – (INFORMATIVE).....	13
10.1 Changes to IEEE 802.1AE-2018 Chapter 7	13
10.2 Changes to IEEE 802.1AE-2018 Chapter 9	13
10.3 Changes to IEEE 802.1AE-2018 Chapter 10	13
10.4 Changes to IEEE 802.1AE-2018 Chapter A.5 Major Capabilities:.....	14
10.5 Changes to IEEE 802.1AE-2018 Chapter A.9.....	14

*OPEN Alliance Specification Copyright Notice and Disclaimer***OPEN SPECIFICATION OWNERSHIP AND USAGE RIGHTS**

As between OPEN Alliance and OPEN Alliance Members whose contributions were incorporated in this OPEN Specification (the “Contributing Members”), the Contributing Members own the worldwide copyrights in and to their given contributions. Other than the Contributing Members’ contributions, OPEN Alliance owns the worldwide copyrights in and to compilation of those contributions forming this OPEN Specification. For OPEN Alliance Members (as that term is defined in the OPEN Alliance Bylaws), OPEN Alliance permits the use of this OPEN Specification on the terms in the OPEN Alliance Intellectual Property Rights Policy and the additional applicable terms below. For non-members of OPEN Alliance, OPEN Alliance permits the use of this OPEN Specification on the terms in the OPEN Alliance Specification License Agreement (available here: <http://www.opensig.org/Automotive-Ethernet-Specifications/>) and the additional applicable terms below. The usage permissions referenced and described here relate only to this OPEN Specification and do not include or cover a right to use any specification published elsewhere and referred to in this OPEN Specification. By using this OPEN Specification, you hereby agree to the following terms and usage restrictions:

RIGHTS AND USAGE RESTRICTIONS SPECIFIC TO OPEN ALLIANCE MEMBERS

FOR OPEN ALLIANCE MEMBERS ONLY: In addition to the usage terms and restrictions granted to Members in the OPEN Alliance Intellectual Property Rights Policy, Members’ use of this OPEN Specification is subject this Copyright Notice and Disclaimer. Members of OPEN Alliance have the right to use this OPEN Specification solely (i) during the term of a Member’s membership in OPEN Alliance and subject to the Member’s continued membership in good standing in OPEN Alliance; (ii) subject to the Member’s continued compliance with the OPEN Alliance governance documents, Intellectual Property Rights Policy, and the applicable OPEN Alliance Promoter or Adopter Agreement, as applicable; and (iii) for internal business purposes and solely to use the OPEN Specification for implementation of this OPEN Specification in the Member’s products and services, but only so long as Member does not distribute, publish, display, or transfer this OPEN Specification to any third party, except as expressly set forth in Section 11 of the OPEN Alliance Intellectual Property Rights Policy. Except and only to the extent required to use this OPEN Specification internally for implementation of this OPEN Specification in Member’s products and services, Member shall not modify, alter, combine, delete portions of, prepare derivative works of, or create derivative works based upon this OPEN Specification. If Member creates any modifications, alterations, or other derivative works of this OPEN Specification as permitted to use the same internally for implementation of this OPEN Specification in

Member's products and services, all such modifications, alterations, or other derivative works shall be deemed part of, and licensed to such Member under the same restrictions as, this OPEN Specification. For the avoidance of doubt, Member shall not include all or any portion of this OPEN Specification in any other technical specification or technical material, product manual, marketing material, or any other material without OPEN Alliance's prior written consent. All rights not expressly granted to Member in the OPEN Alliance Intellectual Property Rights Policy are reserved;

RIGHTS AND USAGE RESTRICTIONS SPECIFIC TO NON-MEMBERS OF OPEN ALLIANCE

FOR NON-MEMBERS OF OPEN ALLIANCE ONLY: Use of this OPEN Specification by anyone who is not a Member in good standing of OPEN Alliance is subject to your agreement to the OPEN Alliance Specification License Agreement (available here: <http://www.opensig.org/Automotive-Ethernet-Specifications/>) and the additional terms in this Copyright Notice and Disclaimer. Non-members have the right to use this OPEN Specification solely (i) subject to the non-member's continued compliance with the OPEN Alliance Specification License Agreement; and (ii) for internal business purposes and solely to use the OPEN Specification for implementation of this OPEN Specification in the non-member's products and services, but only so long as non-member does not distribute, publish, display, or transfer this OPEN Specification to any third party, unless and only to the extent expressly set forth in the OPEN Alliance Specification License Agreement. Except and only to the extent required to use this OPEN Specification internally for implementation of this OPEN Specification in non-member's products and services, non-member shall not modify, alter, combine, delete portions of, prepare derivative works of, or create derivative works based upon this OPEN Specification. If non-member creates any modifications, alterations, or other derivative works of this OPEN Specification as permitted to use the same internally for implementation of this OPEN Specification in non-member's products and services, all such modifications, alterations, or other derivative works shall be deemed part of, and licensed to such non-member under the same restrictions as, this OPEN Specification. For the avoidance of doubt, non-member shall not include all or any portion of this OPEN Specification in any other technical specification or technical material, product manual, marketing material, or any other material without OPEN Alliance's prior written consent. All rights not expressly granted to non-member in the OPEN Alliance Specification License Agreement are reserved.

TERMS APPLICABLE TO BOTH MEMBERS AND NON-MEMBERS OF OPEN ALLIANCE

PATENTS, TRADEMARKS, AND OTHER RIGHTS:

OPEN Alliance has received no Patent Disclosure and Licensing Statements related to this OPEN Specification. Therefore, this OPEN Specification contains no specific disclaimer related to third parties that may require a patent license for their Essential Claims. Having

said that, the receipt of this OPEN Specification shall not operate as an assignment of or license under any patent, industrial design, trademark, or other rights as may subsist in or be contained in or reproduced in this OPEN Specification; and the implementation of this OPEN Specification could require such a patent license from a third party. You may not use any OPEN Alliance trademarks or logos without OPEN Alliance's prior written consent.

Disclaimers and Limitations of Liability:

THIS OPEN SPECIFICATION IS PROVIDED ON AN "AS IS" BASIS, AND ALL REPRESENTATIONS, WARRANTIES, AND GUARANTEES, EITHER EXPLICIT, IMPLIED, STATUTORY, OR OTHERWISE, ARE EXCLUDED AND DISCLAIMED UNLESS (AND THEN ONLY TO THE EXTENT THEY ARE) MANDATORY UNDER LAW. ACCORDINGLY, OPEN ALLIANCE AND THE CONTRIBUTING MEMBERS MAKE NO REPRESENTATIONS OR WARRANTIES OR GUARANTEES WITH REGARD TO THIS OPEN SPECIFICATION OR THE INFORMATION (INCLUDING ANY SOFTWARE) CONTAINED HEREIN. OPEN ALLIANCE AND ALL CONTRIBUTING MEMBERS HEREBY EXPRESSLY DISCLAIM ANY AND ALL SUCH EXPRESS, IMPLIED, STATUTORY, AND ALL OTHER REPRESENTATIONS, WARRANTIES, AND GUARANTEES, INCLUDING WITHOUT LIMITATION ANY AND ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, TITLE, NON-INFRINGEMENT OF OR ABSENCE OF THIRD PARTY RIGHTS, AND/OR VALIDITY OF RIGHTS IN THIS OPEN SPECIFICATION; AND OPEN ALLIANCE AND THE CONTRIBUTING MEMBERS MAKE NO REPRESENTATIONS AS TO THE ACCURACY OR COMPLETENESS OF THIS OPEN SPECIFICATION OR ANY INFORMATION CONTAINED HEREIN. WITHOUT LIMITING THE FOREGOING, OPEN ALLIANCE AND/OR CONTRIBUTING MEMBERS HAS(VE) NO OBLIGATION WHATSOEVER TO INDEMNIFY OR DEFEND YOU AGAINST CLAIMS RELATED TO INFRINGEMENT OR MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS.

OPEN ALLIANCE AND CONTRIBUTING MEMBERS ARE NOT, AND SHALL NOT BE, LIABLE FOR ANY LOSSES, COSTS, EXPENSES, OR DAMAGES OF ANY KIND WHATSOEVER (INCLUDING WITHOUT LIMITATION DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, AND/OR EXEMPLARY DAMAGES) ARISING IN ANY WAY OUT OF USE OR RELIANCE UPON THIS OPEN SPECIFICATION OR ANY INFORMATION HEREIN. NOTHING IN THIS DOCUMENT OPERATES TO LIMIT OR EXCLUDE ANY LIABILITY FOR FRAUD OR ANY OTHER LIABILITY WHICH IS NOT PERMITTED TO BE EXCLUDED OR LIMITED BY OPERATION OF LAW.

COMPLIANCE WITH LAWS AND REGULATIONS:

NOTHING IN THIS DOCUMENT OBLIGATES OPEN ALLIANCE OR CONTRIBUTING MEMBERS TO PROVIDE YOU WITH SUPPORT FOR, OR RELATED TO, THIS OPEN SPECIFICATION OR ANY IMPLEMENTED PRODUCTS OR SERVICES. NOTHING IN THIS OPEN SPECIFICATION CREATES ANY WARRANTIES OR GUARANTEES, EITHER EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, REGARDING ANY LAW OR REGULATION. OPEN ALLIANCE AND CONTRIBUTING MEMBERS EXPRESSLY DISCLAIM ALL LIABILITY, INCLUDING WITHOUT LIMITATION, LIABILITY FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE

OPEN SPECIFICATION OR INFORMATION CONTAINED HEREIN. YOU ARE SOLELY RESPONSIBLE FOR THE COMPLIANCE OF IMPLEMENTED PRODUCTS AND SERVICES WITH ANY SUCH LAWS AND REGULATIONS, AND FOR OBTAINING ANY AND ALL REQUIRED AUTHORIZATIONS, PERMITS, AND/OR LICENSES FOR IMPLEMENTED PRODUCTS AND SERVICES RELATED TO SUCH LAWS AND REGULATIONS WITHIN THE APPLICABLE JURISDICTIONS.

IF YOU INTEND TO USE THIS OPEN SPECIFICATION, YOU SHOULD CONSULT ALL APPLICABLE LAWS AND REGULATIONS. COMPLIANCE WITH THE PROVISIONS OF THIS OPEN SPECIFICATION DOES NOT CONSTITUTE COMPLIANCE TO ANY APPLICABLE LEGAL OR REGULATORY REQUIREMENTS. IMPLEMENTERS OF THIS OPEN SPECIFICATION ARE SOLELY RESPONSIBLE FOR OBSERVING AND COMPLYING WITH THE APPLICABLE LEGAL AND REGULATORY REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, YOU SHALL NOT USE, RELEASE, TRANSFER, IMPORT, EXPORT, AND/OR RE-EXPORT THIS OPEN SPECIFICATION OR ANY INFORMATION CONTAINED HEREIN IN ANY MANNER PROHIBITED UNDER ANY APPLICABLE LAWS AND/OR REGULATIONS, INCLUDING WITHOUT LIMITATION U.S. EXPORT CONTROL LAWS.

Automotive Applications Only:

Without limiting the foregoing disclaimers or limitations of liability in any way, this OPEN Specification was developed for automotive applications only. This OPEN Specification has neither been developed, nor tested for, non-automotive applications.

Right to Withdraw or Modify:

OPEN Alliance reserves the right to (but is not obligated to) withdraw, modify, or replace this OPEN Specification at any time, without notice.

© 2024 OPEN Alliance. This document also contains contents, the copyrights of which are owned by third parties who are OPEN Alliance Contributing Members. Unauthorized Use Strictly Prohibited. All Rights Reserved.

Abbreviation/Symbols

CA	Secure Connectivity Association
CAK	Secure Connectivity Association Key

TERMS AND DEFINITIONS

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

NORMATIVE REFERENCES

The following documents are referred to in the text in such a way that some or all their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[1] IEEE Std 802.1AE™ – 2018, IEEE Standards Association, New York, 2019.

INTRODUCTION

This specification defines an automotive profile and extensions for MACsec based on IEEE 802.1AE-2018 standard. The resulting solution is called “Automotive MACsec”.

The goals for Automotive MACsec include:

- Remove unneeded features and complexity to better fit embedded footprint.
- Add features needed for Automotive use-cases.

These goals are achieved by removing MACsec features, making MACsec features optional and adding new features. This may affect compatibility with regular MACsec implementations. For compatibility, both implementations must be configured to only use common features. Untouched MACsec features of IEEE 802.1AE-2018 standard are not affected and need to be implemented as described in standard.

In this revision, the focus is on “switched Automotive Ethernet” (including 10BASE-T1S in Half Duplex and Full Duplex mode) and not on “Automotive Ethernet Shared Medium” (i.e., 10BASE-T1S in Shared Medium mode). Due to the nature of “10BASE-T1S in Shared Medium mode”, different optimizations and performance targets are required.

The OPEN TC17 10Base-T1S subgroup plans to work on MACsec optimizations for “10BASE-T1S in Shared Medium mode” in a future revision of the document.

1 SCOPE

The following are the objectives of the Automotive MACsec specification:

1. A common MACsec solution for all OEMs
2. Remove features not relevant for Automotive use-cases.
3. Automotive MACsec shall remain interoperable to IEEE MACsec implementation with appropriate configuration. This allows to use the standard test tools.
4. Define specification for “Switched Automotive Ethernet” (including 10BASE-T1S in Half Duplex and Full Duplex mode).
5. Section 2 defines the specifications for Automotive MACsec.
6. Section 3 is informative in nature. Content in this section is to enable easier tracking of changes needed for Automotive MACsec.

2 INTRODUCTION TO AUTOMOTIVE MACSEC – (SPECIFICATIONS)

This document is based on IEEE 802.1AE-2018 standard and uses mechanism defined in the standard.

Requirement AutoMACsec-01001

Automotive MACsec shall support point-to-point MACsec as defined by IEEE 802.1AE 2018.

Note: The optimizations are only designed for point-to-point MACsec. Other or proprietary variations (e.g. end-to-end MACsec) are not considered.

Requirement AutoMACsec-01002

Automotive MACsec shall support at least One Transmit Secure Channel and at least one Receive Secure Channel per Ethernet port.

Requirement AutoMACsec-01003

Automotive MACsec shall be able to function without the support of "IEEE802.3br Frame Pre Emption".

Note: This allows to reduce MACsec hardware complexity and reduced hardware cost.

Requirement AutoMACsec-01004

Automotive MACsec implementation shall support the SecTAG without encoding the SCI (Secure Channel Identifier).

Note : This helps reduce 8 bytes per ethernet frame on the physical layer and enable extra bandwidth for data transfer.

Requirement AutoMACsec-01005

Automotive MACsec shall support following MACsec capabilities:

- Integrity without Confidentiality
- Confidentiality and Integrity with Confidentiality offset 0

Note: Automotive MACsec shall work, when the Offset 30 and Offset 50 are not supported.

Requirement AutoMACsec-01006

Automotive MACsec shall support forwarding of Ethernet packets to Uncontrolled Port based on the atleast following Ethernet frame fields in the Transmit direction.

- MAC DA
- Ethertype
- IEEE802.1Q VLAN tag with matching VLAN ID

Requirement AutoMACsec-01006A

Automotive MACsec shall support forwarding of Ethernet packets to Uncontrolled Port based on atleast following Ethernet frame fields in the Receive direction.

- MAC DA
- Ethertype (applicable to unsecured frames that have Ethertype as not "0x88E5")
- IEEE802.1Q VLAN tag with matching VLAN ID (applicable to unsecured frames that have Ethertype as not "0x88E5")

Requirement AutoMACsec-01006B

It shall be possible to have at least 8 different rules with flexibility to use these rules in Transmit and/or Receive direction.

Requirement AutoMACsec-01007

Automotive MACsec shall perform frame verification as per 802.1AE 2018. If MACsec is not able to drop the frame for failed frame verification (e.g. authentication failure), it shall forward the Ethernet frame with FCS corrupted.

Requirement AutoMACsec-01008

Automotive MACsec shall at least support maintenance of the following statistics/counters

- Out: tx_secy_statistics (from IEEE 802.1AE SecyStatsEntry, TX part):
 - uint64 out_pkts_untagged. OutPktsUntagged as per [1AE] Section 10.7.18
 - uint64 out_pkts_too_long. OutPktsTooLong as per [1AE] Section 10.7.18
 - uint64 out_octets_protected. OutPktsProtected as per [1AE] Section 10.7.19
 - uint64 out_octets_encrypted. OutPktsEncrypted as per [1AE] Section 10.7.19
- Out: rx_secy_statistics (from IEEE 802.1AE SecyStatsEntry, RX part):
 - uint64 in_pkts_untagged. InPktsUntagged as per [1AE] Section 10.7.9
 - uint64 in_pkts_no_tag. InPktsNoTag as per [1AE] Section 10.7.9.
 - uint64 in_pkts_bad_tag. InPktsBadTag as per [1AE] Section 10.7.9.
 - uint64 in_pkts_no_sa. InPktsNoSA as per [1AE] Section 10.7.9.
 - uint64 in_pkts_no_sa_error. InPktsNoSAError as per [1AE] Section 10.7.9.
 - uint64 in_pkts_overrun. InPktsOverrun as per [1AE] Section 10.7.9.
 - uint64 in_octets_validated. InOctetsValidated, as per [1AE] Section 10.7.10.
 - uint64 in_octets_decrypted. InOctetsDecrypted, as per [1AE] Section 10.7.10.
- Out: tx_sc_statistics: 0..n array of tx_sc_statistics_entry (see [1AE] secyTxSCStatsEntry):
 - uint64 out_pkts_protected. OutPktsProtected as per [1AE] Section 10.7.18.
 - uint64 out_pkts_encrypted. OutPktsEncrypted as per [1AE] Section 10.7.18.
- Out: rx_sc_statistics: 0..n array of rx_sc_statistics_entry (see [1AE] secyRxSCStatsEntry):
 - uint64 in_pkts_ok. InPktsOK as per [1AE] Section 10.7.9.
 - uint64 in_pkts_unchecked. InPktsUnchecked as per [1AE] Section 10.7.9.
 - uint64 in_pkts_late. InPktsLate as per [1AE] Section 10.7.9.
 - uint64 in_pkts_invalid. InPktsInvalid as per [1AE] Section 10.7.9.
 - uint64 in_pkts_not_valid. InPktsNotValid as per [1AE] Section 10.7.9.

3 CHANGES TO IEEE 802.1AE-2018 – (INFORMATIVE)

The following chapters refer directly to the IEEE 802.1AE-2018 chapters concerning MACsec. While this duplicates information, it makes it easier for implementers to understand the proposed changes as they can compare with the original standard.

3.1 Changes to IEEE 802.1AE-2018 Chapter 7

Section 7.1. Secure Channels :

Requirement AutoMACsec-01002 defines the number of Secure channel (SC) needed per Ethernet port for Automotive MACsec

3.2 Changes to IEEE 802.1AE-2018 Chapter 9

Section 9.3 MAC Security TAG

Requirement AutoMACsec-01004 defines optional SCI need for Automotive MACsec

3.3 Changes to IEEE 802.1AE-2018 Chapter 10

Section 10.1 SECY Overview

Requirement AutoMACsec-01006, AutoMACsec-01006A, AutoMACsec-01006B defines the rules for forwarding routing the frames to uncontrol ported:

Section 10.6 Secure frame Verification

Requirement AutoMACsec-01007 allows received frames failing secure frame verification to be output with FCS corruption.

Section 10.7.16 Frame generation Capabilities

Requirement AutoMACsec-01002 defines the number of Secure channel (SC) needed per Ethernet port for Automotive MACsec

Requirement AutoMACsec-01003: defines Automotive MACsec shall operate without support of 802.3br.

Section 10.7.25:

Confidentiality Offset is supported as per **AutoMACsec-01005**

This pre filled PICS would specify, in 802.1AE-2018 language, the AutoMACsec profile, by defining with yes/no, on each entry, what is supported and what is not supported to be compliant to AutoMACsec profile and, also, the deviation of the AutoMACsec profile from the IEEE802.

3.4 Changes to IEEE 802.1AE-2018 Chapter A.5 Major Capabilities:

	Need to comply to Automotive MACsec/MKA Requirement	
PERF	Requirement AutoMKA-xxx	
MSC	Requirement AutoMACsec-01002	
MSAK	Requirement AutoMACsec-01003	
CSO	Requirement AutoMACsec-01005	
CSRC	Requirement AutoMACsec-01002	
TC	No	
TCT	No	
TCAPT	No	

3.5 Changes to IEEE 802.1AE-2018 Chapter A.9

VER-6	Frame Discarded or Requirement AutoMACsec-01007	
-------	---	--