Document Title	Requirements on MACsec
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	1065

Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R22-11

Document Change History			
Date	**Release**	**Changed by**	**Description**
2022-11-24	R22-11	AUTOSAR Release Management	• Initial release

Disclaimer

Contents

1 Scope of Document

This document specifies requirements on MACsec protocols in the AUTOSAR Foundation. The motivation is to specify the usage of:

- IEEE 802.1AE (also known as MACsec) protocol.
- MACsec Key Agreement protocol (standardized in IEEE 802.1X).

2 Conventions to be used

2.1 Document Conventions

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see Standardization Template, chapter Support for Traceability ([1]).

The verbal forms for the expression of obligation specified in [TPS_STDT_00053] shall be used to indicate requirements, see Standardization Template, chapter Support for Traceability ([1]).

2.2 Requirements Guidelines

2.2.1 Requirements quality

No content.

2.2.2 Requirements identification

No content.

2.2.3 Requirements status

No content.

3 Acronyms and abbreviations

The glossary below includes acronyms and abbreviations relevant to this document that are not included in the AUTOSAR Glossary [2].

Abbreviation / Acronym:	Description:
AN	Association Number
CA	Secure Connectivity Association
CAK	Secure Connectivity Association Key
DA	Destination Address
ICV	Integrity Check Value
KaY	MAC Security Key Agreement Entity
MACsec	Media Access Control Security
MKA	MACsec Key Agreement protocol (IEEE Std 802.1X)
MKPDU	MACsec Key Agreement Protocol Data Unit
MPDU	MACsec Protocol Data Unit
PAE	Port Access Entity
PN	Packet Number
SA	Secure Association or Source Address, as applicable
SAI	Secure Association Identifier
SAK	Secure Association Key
SC	Secure Channel
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SL	Short Length
SSCI	Short Secure Channel Identifier

Table 3.1: Acronyms and abbreviations used in the scope of this Document

4 Requirements Specification

This chapter describes all requirements driving the work to define the MACsec protocols.

4.1 Functional Overview

IEEE 802.1AE (also known as MACsec) is a network security standard that operates at the medium access control layer and defines connectionless data confidentiality and integrity for media access independent protocols.

The 802.1AE standard specifies the implementation of MAC Security Entities (SecY), which are part of the stations attached to the same LAN, providing secure MAC service to the client. The standard defines:

- MACsec frame format, which is a valid Ethernet frame with a specific EtherType and includes the following additional fields:
  - Security Tag, which is an extension of the EtherType.
  - Message authentication code (ICV).
- Secure Connectivity Associations (CAs) that represent groups of stations connected via unidirectional Secure Channels.
- Security Associations (SAs) within each Secure Channel. Each association uses its own key (SAK). More than one association is permitted within the channel for the purpose of key change without traffic interruption (standard requires devices to support at least two).
- A default cipher suite of GCM-AES-128 (Galois/Counter Mode of Advanced Encryption Standard cipher with 128-bit key)
  - GCM-AES-256 using a 256-bit key is supported

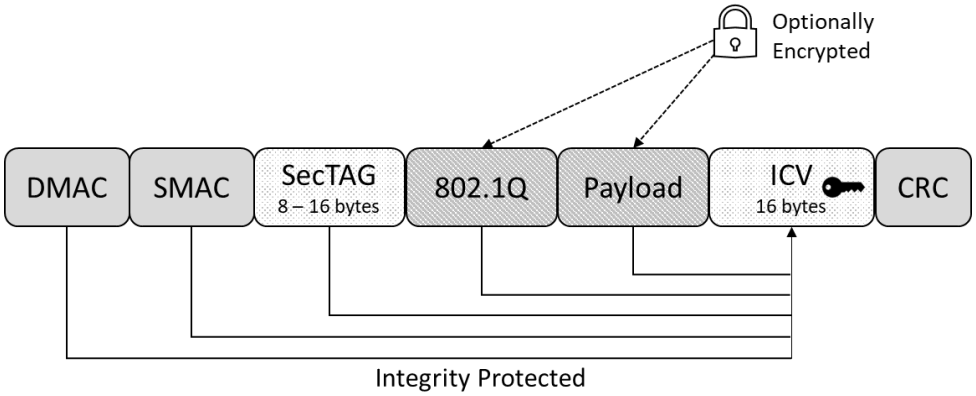

Figure 4.1: MACsec frame layout

MACsec allows unauthorized LAN connections to be identified and excluded from communication within the network. In common with IPsec and TLS, MACsec defines a security infrastructure to provide data confidentiality, data integrity, and data origin authentication.

By assuring that a frame comes from the station that claimed to send it (this might require additional mechanisms), MACsec can even mitigate attacks on Layer 2 protocols that cannot be protected otherwise. A scenario in which MACsec protects a layer 2 attack, is in case an intruder installs a device in the cable harness to launch a man-in-the-middle attack.

In order to recognize participants belonging to the same Secure Connectivity Association (CAs), establish Secure Channels, and maintain them alive, the participants on the communication make use of the MACsec Key Agreement protocol (MKA). This protocol is described and specified in the IEEE 802.1X standard.

4.1.1 Motivation

AUTOSAR supports actually several protocols to establish a secure communication channel which provide data confidentiality, data integrity and data origin authentication over Ethernet (e.g. IPsec, TLS, SecOC).

The TLS protocol aims primarily to provide privacy and data integrity between two communication peers. If more than two communication peers need to exchange data in integrity protected way, for each peer connection an own TLS connection must be setup. TLS is application protocol independent; higher-level protocols can layer on top of TLS transparently. TLS needs for each application-based session an own setup connection, which leads to a resource overhead. Each session needs an own database entry for the negotiated key, the session status, and other organizational information.

To avoid the overhead introduced by the large number of required TLS connections it is possible to push the secure communication channel one level down, to the IP layer. To secure the IP layer IPsec was introduced. IPsec includes protocols for establishing mutual authentication between hosts at the beginning of a session and negotiation of cryptographic keys to use during the session. IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. It supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection (RFC 4301).

The advantage of IPsec, compared to TLS, is the reduced overhead, because IPsec combines all secure application channels to a single secure channel. However, IPsec has a negative impact in the typical automotive use case. Since IPsec connects on a host-to-host level and in the automotive world it is sometimes not possible to use

the Internet model, as the connectivity between hosts is higher. Here, the numbers of connections will also increase the resources and key negotiations time by power of two when an additional peer joins the secure communication network. Avoiding this overhead again is possible pushing the secure channel one level down, to the MAC layer. With security on the MAC layer, protocols not based on IP as well as protocols using multicast can be protected.

The goal is to introduce the IEEE 802.1AE (MACsec) solution to reduce overhead in a meshed network layout and to reduce the timing issue during key negotiation by reducing the number of peers (peer per Ethernet port instead of peer per UDP/TCP port) and avoiding higher network stack layers.

Implementing the MACsec protocol in the AUTOSAR platform provides options to establish secure communication channels between network nodes with confidentiality and/or integrity. This document deals with the realization of the functionality either in a MACsec aware hardware (PHY or specific controller) and MACsec software solution, and the interoperability of the different solutions with each other.

In the AUTOSAR Classic Platform an adaption of the MAC layer is needed to implement the IEEE 802.1AE solution.

4.1.2 Functional elements

The standards related with MACsec ([3, IEEE-802.1AE-2018] and [4, IEEE-802.1X-2020]) define the following functional elements:

- MAC Security Entities (SecYs): The SecY defines and identifies the authentic partners. A SecY implements the secure MAC Service to its clients. The MAC Security Entity is responsible of integrity protecting/validating and, if required, encrypt/decrypt to provide user data confidentiality. The SecY can be a SW or a HW implementation.
- Port Access Entities (PAEs): The PAE provides mutual authentication of participants belonging to a secure Connectivity Association (CA), and agrees the cryptographic keys and related parameters to meet the requirements of the SecY.
- MAC Security Key Agreement Entities (KaYs): The KaY is the responsible for MKA within the PAE, it serves to setup a Secure Channel via a key agreement and monitors it during its life cycle.
- Secure Channel (SC): Stores various configuration parameters, such as whether to perform replay protection, or whether to enable encryption.
- Secure Association (SA): Security relationship under a Secure Channel. Each SA supports a different key. A Secure Channel supports several consecutive SAs to allow exchanging Keys without terminating the established Secure Channel.
- MKPDU: MACsec Key Agreement Protocol Data Units.

- MACsec Protocol Data Units (MPDU): Defines the frame layout, which resides in the MAC layer (ISO/OSI layer 2).

The following terms identify roles within the protocol scenarios:

- Participant: The personification of a single KaY's participation in a given MKA instance. It transmits and receives MKPDUs protected by keys derived from a single given CAK and identified by a Connectivity Association Key Name (CKN).
- Key Server: Authenticated participant which generates and distributes the Secure Association Key to use in a Secure Channel. This participant decides the cipher suites to use.
- Peer: Authenticated participant which does not possess the Key Server role.

The following keys are required for the MACsec and MKA communication:

- Secure Connectivity Association Key (CAK): Secret key possessed by members of a given CA. The CAK is identified by its respective secure Connectivity Association Key Name (CKN).
- Integrity Check Value Key (ICK): Key derived from the respective CAK and used to transmit/validate Integrity protected MKPDUs.
- Key Encrypting Key (KEK): Key derived from the respective CAK and used to encrypt/decrypt a Secure Association Key (SAK).
- Secure Association Key (SAK): Key used by the MACsec Entity (SecY) to integrity protect/validate and/or encrypt/decrypt MPDUs belonging to an specific Secure Association. The SAK is generated by one MKA participant (Key Server) and distributed during the MKA sequence.

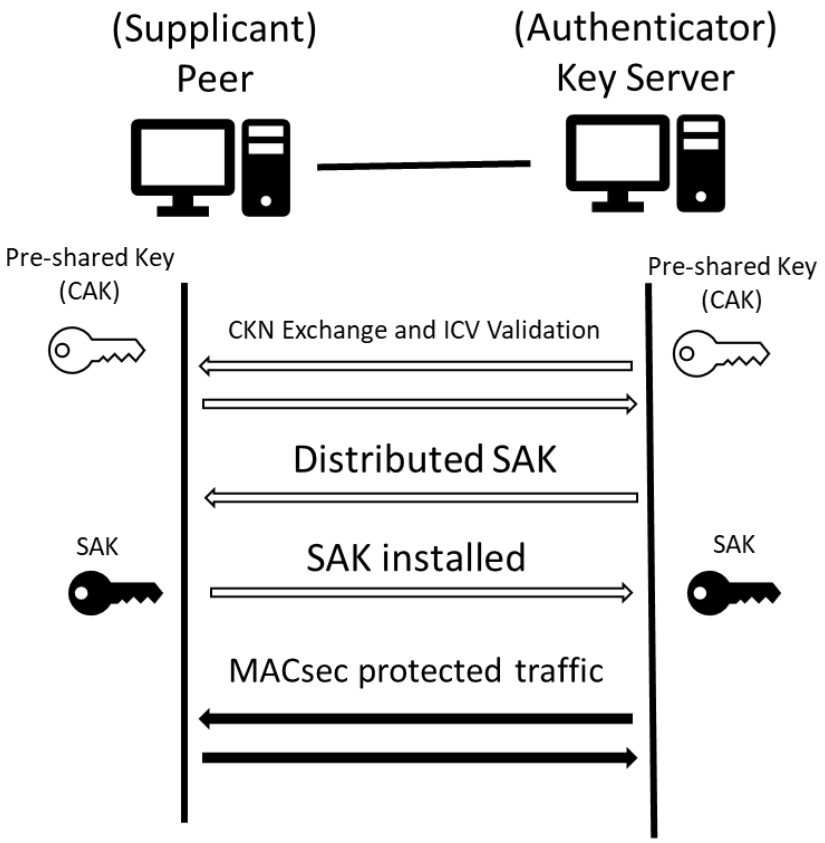

Figure 4.2: MACsec Key Agreement sequence with pre-shared key

As depicted in Figure 4.2, the MKA protocol consists of three phases:

1. Authentication of participants.
2. Session negotiation.
3. Secure communication.

4.1.2.1 Authentication of participants

During the first phase of the MKA sequence, the MKA Entity (KaY) identifies other participants belonging to its configured CA.
In the current version of this document, only pre shared keys authentication is supported and the participants possess fixed roles in the MKA sequence.
The participants of the MKA communication will identify and authenticate each other based on the CKN and ICV of the MKPDUs exchanged. Once a participant can successfully identify and authenticate another participant belonging to the same CA, the member identifier of the other participant is included in its transmitted “Potential Peer List”.

If a participant recognizes another one and it is listed in the others “Potential peer List”, it will mark it as Live participant. The Member Identifier of the other participant will be included in the transmitted “Live Peer List”.

4.1.2.2 Session negotiation

In the current version of this document, dynamic election of the Key Server member is not supported, and therefore each participant will currently configure in advance its role in the communication.

The participants can share the supported cipher suites by means of the “MACsec Cipher Suites Announcement”. The participant with the Key Server role will select a cipher suite and generate and distribute a Secure Association Key accordingly.

Both participants shall communicate the readiness to transmit and receive MACsec protected PDUs with the “MACsec SAK Use” parameter set.

During the Secure Channel life time, it is possible to distribute new SAKs (and therefore create a new SA) without a communication interruption. The participants can also detect if the communication partner is alive.

In case a cipher suite with Extended Packet Number (XPN) is selected, additional parameter sets are exchanged during the Secure Channel life time to keep the channel information up-to-date.

4.1.2.3 Secure communication

After the identification, mutual authentication, distribution of keys, and installation of keys, the secure communication can start based on the parameters exchanged in the previous phases.

4.2 Functional Requirements

4.2.1 Standards to support

[FO_RS_MACsec_00001]{DRAFT} **MACsec Protocol support** ⌈

Description:	MACsec shall be supported as specified in [3, IEEE-802.1AE-2018]
Rationale:	To enable secure communication over MAC
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE

▽

△

AppliesTo:	CP, AP

⌋(*RS_Main_00280*, *RS_Main_00510*, *RS_Main_00514*)

[FO_RS_MACsec_00002]{DRAFT} **MACsec Key Agreement Protocol support** ⌈

Description:	MACsec Key Agreement (MKA) shall be supported as specified in [4, IEEE-802.1X-2020] The MKA version to use shall be version 3.
Rationale:	To enable secure communication over MAC
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1X
AppliesTo:	CP, AP

⌋(*RS_Main_00280*, *RS_Main_00510*, *RS_Main_00514*)

4.2.2 Common Requirements

[FO_RS_MACsec_00003]{DRAFT} **Using MACsec on external communication links** ⌈

Description:	The implementation of MKA shall be able to send and receive MKA traffic as defined in [4, IEEE-802.1X-2020]. The implementation shall be able to monitor and configure MACsec operation following [3, IEEE-802.1AE-2018] on or through all selected external ports, i.e., ports connecting to other peers. The selection of ports to use MKA upon shall be realized via configuration.
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE, IEEE 802.1X
AppliesTo:	CP, AP

⌋(*RS_Main_00280*, *RS_Main_00510*, *RS_Main_00514*)

[FO_RS_MACsec_00004]{DRAFT} **Configure which Ethernet ports use MACsec** ⌈

Description:	The configuration of which Ethernet port uses MACsec shall be supported.
Rationale:	Allow to select which Ethernet ports are MACsec protected and which are unprotected.
Dependencies:	–
Use Case:	In-vehicle secure communication

▽

△

Supporting Material:	–
AppliesTo:	CP, AP

⌋(*RS_Main_00510*, *RS_Main_00514*)

[FO_RS_MACsec_00005]{DRAFT} **MACsec status control** ⌈

Description:	The implementation of MKA shall provide an option to control the MACsec state of the interfaces. Activation, deactivation of MACsec on a network interface.
Rationale:	Activation and deactivation of MACsec.
Dependencies:	–
Use Case:	Control of the MACsec status during production or maintenance.
Supporting Material:	IEEE 802.1X
AppliesTo:	CP, AP

⌋(*RS_Main_00510*, *RS_Main_00514*)

[FO_RS_MACsec_00006]{DRAFT} **MACsec support for Adaptive AUTOSAR Platform** ⌈

Description:	The Adaptive AUTOSAR Platform's Operating System shall provide mechanisms to configure the MACsec related resources.
Rationale:	In order to assure the correct setup and configuration of MACsec within Adaptive AUTOSAR Platform according to [3, IEEE-802.1AE-2018] and [4, IEEE-802.1X-2020] Standards.
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	–
AppliesTo:	AP

⌋(*RS_Main_00510*, *RS_Main_00514*)

[FO_RS_MACsec_00007]{DRAFT} **Configuration of unprotected traffic (for Software-based MACsec)** ⌈

Description:	The MACsec Entity shall provide a mechanism to configure rules to bypass MACsec for incoming and outgoing traffic based on EtherType and/or VLAN-ID. All traffic not configured as bypassed traffic shall be processed by the MACsec entity or dropped. This configuration shall be supported at initial configuration time of the ports.
Rationale:	Enables the ports to support secure and insecure communication simultaneously.
Dependencies:	–
Use Case:	Simultaneous In-vehicle secure and insecure communication

▽

△

Supporting Material:	–
AppliesTo:	CP, AP

⌋(*RS_Main_00510, RS_Main_00514*)

[FO_RS_MACsec_00008]{DRAFT} **Configuration of unprotected traffic (for Hardware-based MACsec)** ⌈

Description:	The MACsec capable HW shall provide a mechanism to configure rules to bypass MACsec for incoming and outgoing traffic based on EtherType and/or VLAN-ID. All traffic not configured as bypassed traffic shall be processed by the MACsec Entity or dropped. This configuration shall be supported at initial configuration time of the Transceiver, Eth Controller, and Switch.
Rationale:	Enables the ports to support secure and insecure communication simultaneously.
Dependencies:	–
Use Case:	Simultaneous In-vehicle secure and insecure communication
Supporting Material:	–
AppliesTo:	CP, AP

⌋(*RS_Main_00510, RS_Main_00514*)

[FO_RS_MACsec_00009]{DRAFT} **MACsec Security Events** ⌈

Description:	All MACsec Entities (SW or HW) shall support status counters for the following information, which may be attached to IDSM functionality: • Dropped frames because of incorrect ICV per port. • Unsuccessful MKA sequence per peer. • Additionally all the port statistics required by [3, IEEE-802.1AE-2018].
Rationale:	Monitoring of the MACsec channels statuses and statistics.
Dependencies:	–
Use Case:	Monitoring of the MACsec channels statuses and statistics.
Supporting Material:	[5, RS_IntrusionDetectionSystem], [3, IEEE-802.1AE-2018]
AppliesTo:	CP, AP

⌋(*RS_Main_00491*)

4.2.3 Requirements on MACsec Protocol

[FO_RS_MACsec_00010]{DRAFT} **Support of integrity and confidentiality** ⌈

Description:	The MACsec Entity (SW or HW) shall support "Integrity only" as well as "Integrity with Confidentiality" for all supported ciphers.
Rationale:	Configurable protection depending on needs.
Dependencies:	–
Use Case:	Integrity protection or confidentiality support for links.
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00011]{DRAFT} **MAC Security TAG** ⌈

Description:	MACsec Entity (SW or HW) shall support MAC Security TAG (SecTAG) as defined in [3, IEEE-802.1AE-2018]. The SecTAG shall convey: • TAG Control Information (TCI) • Association Number (AN) • Short Length (SL) • Packet Number (PN) • Secure Channel Identifier (SCI) - Optional
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00012]{DRAFT} **MACsec EtherType** ⌈

Description:	MACsec Entity (SW or HW) shall support MACsec EtherType as defined in [3, IEEE-802.1AE-2018].
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00017]{DRAFT} **Support of Extended Packet Number (XPN)** ⌈

Description:	MKA module and MACsec Entity (SW or HW) shall support Extended Packet Number (XPN) as defined in [3, IEEE-802.1AE-2018]. The XPN extends the PN to 64 bits.
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00018]{DRAFT} **Secure Channel Identifier (SCI)** ⌈

Description:	The MKA module and MACsec Entity (SW or HW) shall support Secure Channel Identifier (SCI), as defined in [3, IEEE-802.1AE-2018]. The SCI may be encoded in the SecTAG if SCI is required to be sent.
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00019]{DRAFT} **Secure Data** ⌈

Description:	MACsec Entity (SW or HW) shall support Secure Data as defined in [3, IEEE-802.1AE-2018].
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00020]{DRAFT} **Integrity Check Value (ICV)** ⌈

Description:	MACsec Entity (SW or HW) shall support Integrity Check Value (ICV) as defined in [3, IEEE-802.1AE-2018]. The ICV length depends on the used cipher suite but is not less than 8 octets and not more than 16 octets. Note that with the currently supported cipher suites, the transmitted ICV is always 16 octets.
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00021]{DRAFT} **Protect function in software solution** ⌈

Description:	MACsec Entity (SW) shall support a protect function as specified in [3, IEEE-802.1AE-2018].
Rationale:	Valid in case Software based MACsec configuration is needed.
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00022]{DRAFT} **Validation function in software solution** ⌈

Description:	MACsec Entity (SW) shall support a validation function as specified in [3, IEEE-802.1AE-2018].
Rationale:	Valid in case software based MACsec configuration is needed.
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

4.2.4 Requirements on MKA Protocol

[FO_RS_MACsec_00023]{DRAFT} **Support of MKA Packets** ⌈

Description:	The MKA implementation shall support the Port Access Entity EtherType and the MACsec Key Agreement (MKA) Packet Type as defined in [4, IEEE-802.1X-2020].
Rationale:	Support of MKA
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1X
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00024]{DRAFT} **Pre-shared key support** ⌈

Description:	The MKA implementation shall support standardized authentication based on a Connectivity Association pre-shared key (CAK).
Rationale:	Support of MKA
Dependencies:	–
Use Case:	Authentication of participants based on pre-shared keys.
Supporting Material:	[4, IEEE-802.1X-2020]
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00025]{DRAFT} **Key selection via CKN** ⌈

Description:	It shall be possible to select the CAK and/or derived keys (i.e. ICK and KEK) using the CKN transported in MKA by the peer.
Rationale:	Authentication of participants based on pre-shared keys.
Dependencies:	–
Use Case:	Mutual authentication of participants.
Supporting Material:	[4, IEEE-802.1X-2020]
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

4.2.5 Cryptography for MACsec and MKA

[FO_RS_MACsec_00026]{DRAFT} **GCM-based cipher support** ⌈

Description:	The MACsec implementation shall support the GCM-based ciphers as defined in [3, IEEE-802.1AE-2018].
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00027]{DRAFT} **Support of AES ciphers with at least 128 bits of key length** ⌈

Description:	The MACsec implementation shall support AES ciphers with at least 128 bits of key length.
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00028]{DRAFT} **Support of AES ciphers with 256 bits of key length** ⌈

Description:	The MACsec implementation shall support AES ciphers with 256 bits of key length.
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00029]{DRAFT} **Support of Key Encryption Key (KEK)** ⌈

Description:	The MKA implementation shall support a KEK per MKA instance. The KEK is derived from the Connectivity Association Key (CAK) by using the Key Derivation Function as defined in [4, IEEE-802.1X-2020].
Rationale:	Support of MKA
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1X, RFC 3394
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00030]{DRAFT} **Support of Integrity Check Value Key (ICK)** ⌈

Description:	The MKA implementation shall support an ICK per MKA instance. The ICK is derived from the Connectivity Association Key (CAK) by using the Key Derivation Function as defined in [4, IEEE-802.1X-2020].
Rationale:	Support of MKA
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1X, RFC 3394
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00031]{DRAFT} **Support of Key Derivation Function (KDF)** ⌈

Description:	The MKA implementation shall use the Key Derivation Function as defined in [4, IEEE-802.1X-2020] and [6, RFC 3394], which uses an AES Cipher in CMAC mode [7, RFC 4493].
Rationale:	Support of MKA
Dependencies:	In case of CP: [8, AUTOSAR_RS_Cryptography]
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1X, RFC 3394, RFC 4493
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00032]{DRAFT} **List of minimal supported cipher suites** ⌈

Description:	MACsec Entity (SW or HW) shall support the following ciphers suites: • GCM-AES-128 • GCM-AES-256 • GCM-AES-XPN-128 • GCM-AES-XPN-256 GCM-AES is the standard algorithm for MACsec in [3, IEEE-802.1AE-2018].
Rationale:	Support of MACsec
Dependencies:	In case of CP: [8, AUTOSAR_RS_Cryptography]
Use Case:	In-vehicle secure communication, Adaption of cipher-suite based on resources
Supporting Material:	IEEE 802.1AE, IEEE 802.1X
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00033]{DRAFT} **Validation function for ICVs** ⌈

Description:	The MACsec Entity (HW or SW) and MKA implementation shall support a validation function for MACsec and MKA ICVs respectively.
Rationale:	Support of MACsec and MKA
Dependencies:	In case of CP: [8, AUTOSAR_RS_Cryptography]
Use Case:	In-vehicle secure communication, Authentication of participants
Supporting Material:	IEEE 802.1AE, IEEE 802.1X
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00034]{DRAFT} **Generation function for ICVs** ⌈

Description:	The MACsec Entity (HW or SW) and MKA implementation shall support a generation function for MACsec and MKA ICVs respectively.
Rationale:	Support of MACsec and MKA
Dependencies:	In case of CP: [8, AUTOSAR_RS_Cryptography]
Use Case:	In-vehicle secure communication, Authentication of participants
Supporting Material:	IEEE 802.1AE, IEEE 802.1X
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

[FO_RS_MACsec_00035]{DRAFT} **Key Handling with combined HSM and MACsec functionality** ⌈

Description:	It shall be supported that -on supporting hardware- session keys (SAKs) protected by AES Key Wrap can directly be installed from a HSM to a MACsec Entity (SecY).
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	[6, RFC 3394]
AppliesTo:	CP, AP

⌋*(RS_Main_00514)*

4.2.6 Requirements for MACsec capable hardware

[FO_RS_MACsec_00036]{DRAFT} **Interframe gap configuration of Ethernet controller** ⌈

Description:	Systems with MACsec implemented by an external physical layer chip shall allow adjusting the interframe gap, to accommodate the additional MACsec SecTAG (8-16 bytes) and ICV (16 bytes as specified in [3, IEEE-802.1AE-2018]).
Rationale:	Support of MACsec
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IEEE 802.1AE
AppliesTo:	CP, AP

⌋*(RS_Main_00280, RS_Main_00510, RS_Main_00514)*

4.2.7 Additions to Standards

[FO_RS_MACsec_00037]{DRAFT} **MACsec participants per link** ⌈

Description:	The MKA implementation shall assume exactly two participants per link. Therefore, having exactly one peer.
Rationale:	This requirement permits a KaY instance to immediately continue with the MKA sequence after detecting an successfully authenticating another participant in the link, avoiding start-up delays.
Dependencies:	–

▽

△

Use Case:	In-vehicle secure communication
Supporting Material:	–
AppliesTo:	CP, AP

⌋(*RS_Main_00280*, *RS_Main_00510*, *RS_Main_00514*)

[FO_RS_MACsec_00038]{DRAFT} **MKA SC establishment retry phase** ⌈

Description:	The MKA implementation shall support retry for the MKA sequence. If a KaY instance cannot successfully identify or successfully establish a SC with any participant in the Link, it should retry the MKA sequence following a per configuration parametrized *retry base delay with Exponential Back-off* until a *retry cyclic delay* in ms. (e.g. 20ms, 40ms, 80ms, 160ms, 320ms, 500ms, 500ms, ...).
Rationale:	Delayed start-up times of participants
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	–
AppliesTo:	CP, AP

⌋(*RS_Main_00280*, *RS_Main_00510*, *RS_Main_00514*)

[FO_RS_MACsec_00039]{DRAFT} **MKA rekey conditions** ⌈

Description:	The MKA implementation shall support rekey of SAKs as specified in [4, IEEE-802.1X-2020] and additionally in any of the following conditions: • After a configurable time span. • If the Packet Number space of one direction (reception and/or transmission) is more than 80% used.
Rationale:	Configurable SAK rekey conditions.
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	–
AppliesTo:	CP, AP

⌋(*RS_Main_00280*, *RS_Main_00510*, *RS_Main_00514*)

4.3 Non-Functional Requirements (Qualities)

No content.

5 Requirements Tracing

The following table references the features specified in [9] and links to the fulfillments of these.

Requirement	Description	Satisfied by
[RS_Main_00280]	Standardized Automotive Communication Protocols	[FO_RS_MACsec_00001] [FO_RS_MACsec_00002] [FO_RS_MACsec_00003] [FO_RS_MACsec_00010] [FO_RS_MACsec_00011] [FO_RS_MACsec_00012] [FO_RS_MACsec_00017] [FO_RS_MACsec_00018] [FO_RS_MACsec_00019] [FO_RS_MACsec_00020] [FO_RS_MACsec_00021] [FO_RS_MACsec_00022] [FO_RS_MACsec_00023] [FO_RS_MACsec_00024] [FO_RS_MACsec_00025] [FO_RS_MACsec_00026] [FO_RS_MACsec_00027] [FO_RS_MACsec_00028] [FO_RS_MACsec_00029] [FO_RS_MACsec_00030] [FO_RS_MACsec_00031] [FO_RS_MACsec_00032] [FO_RS_MACsec_00033] [FO_RS_MACsec_00034] [FO_RS_MACsec_00036] [FO_RS_MACsec_00037] [FO_RS_MACsec_00038] [FO_RS_MACsec_00039]
[RS_Main_00491]	Function Monitoring	[FO_RS_MACsec_00009]
[RS_Main_00510]	Secure Onboard Communication	[FO_RS_MACsec_00001] [FO_RS_MACsec_00002] [FO_RS_MACsec_00003] [FO_RS_MACsec_00004] [FO_RS_MACsec_00005] [FO_RS_MACsec_00006] [FO_RS_MACsec_00007] [FO_RS_MACsec_00008] [FO_RS_MACsec_00010] [FO_RS_MACsec_00011] [FO_RS_MACsec_00012] [FO_RS_MACsec_00017] [FO_RS_MACsec_00018] [FO_RS_MACsec_00019] [FO_RS_MACsec_00020] [FO_RS_MACsec_00021] [FO_RS_MACsec_00022] [FO_RS_MACsec_00023] [FO_RS_MACsec_00024] [FO_RS_MACsec_00025] [FO_RS_MACsec_00026] [FO_RS_MACsec_00027] [FO_RS_MACsec_00028] [FO_RS_MACsec_00029] [FO_RS_MACsec_00030] [FO_RS_MACsec_00031] [FO_RS_MACsec_00032] [FO_RS_MACsec_00033] [FO_RS_MACsec_00034] [FO_RS_MACsec_00036] [FO_RS_MACsec_00037] [FO_RS_MACsec_00038] [FO_RS_MACsec_00039]
[RS_Main_00514]	System Security Support	[FO_RS_MACsec_00001] [FO_RS_MACsec_00002] [FO_RS_MACsec_00003] [FO_RS_MACsec_00004] [FO_RS_MACsec_00005] [FO_RS_MACsec_00006] [FO_RS_MACsec_00007] [FO_RS_MACsec_00008] [FO_RS_MACsec_00010] [FO_RS_MACsec_00011] [FO_RS_MACsec_00012] [FO_RS_MACsec_00017] [FO_RS_MACsec_00018] [FO_RS_MACsec_00019] [FO_RS_MACsec_00020] [FO_RS_MACsec_00021] [FO_RS_MACsec_00022] [FO_RS_MACsec_00023] [FO_RS_MACsec_00024] [FO_RS_MACsec_00025] [FO_RS_MACsec_00026] [FO_RS_MACsec_00027] [FO_RS_MACsec_00028] [FO_RS_MACsec_00029] [FO_RS_MACsec_00030] [FO_RS_MACsec_00031] [FO_RS_MACsec_00032] [FO_RS_MACsec_00033] [FO_RS_MACsec_00034] [FO_RS_MACsec_00035] [FO_RS_MACsec_00036] [FO_RS_MACsec_00037] [FO_RS_MACsec_00038] [FO_RS_MACsec_00039]

Table 5.1: RequirementsTracing

6 References

[1] Standardization Template
AUTOSAR_TPS_StandardizationTemplate

[2] Glossary
AUTOSAR_TR_Glossary

[3] IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security
https://ieeexplore.ieee.org/document/8585421

[4] IEEE Standard for Local and Metropolitan Area Networks–Port-Based Network Access Control
https://ieeexplore.ieee.org/document/9018454

[5] Requirements on Intrusion Detection System
AUTOSAR_RS_IntrusionDetectionSystem

[6] Advanced Encryption Standard (AES) Key Wrap Algorithm
https://tools.ietf.org/html/rfc3394

[7] The AES-CMAC Algorithm
https://www.rfc-editor.org/info/rfc4493

[8] Requirements on Cryptography
AUTOSAR_RS_Cryptography

[9] Requirements on AUTOSAR Features
AUTOSAR_RS_Features

6.1 Related standards and norms

6.1.1 IEEE

1. IEEE 802.1AE-2018 Media Access Control (MAC) Security (v.2018)
2. IEEE 802.1X-2020 Port-Based Network Access Control (v.2020)