| Document Title | Explanation of MACsec and MKA Protocols implementation and configuration guidelines |
|---|---|
| **Document Owner** | AUTOSAR |
| **Document Responsibility** | AUTOSAR |
| **Document Identification No** | 1067 |

| | |
|---|---|
| **Document Status** | published |
| **Part of AUTOSAR Standard** | Adaptive Platform |
| **Part of Standard Release** | R24-11 |

**Document Change History**

| Date | Release | Changed by | Description |
|---|---|---|---|
| 2024-11-27 | R24-11 | AUTOSAR Release Management | • Editorial changes |
| 2023-11-23 | R23-11 | AUTOSAR Release Management | • Initial release |

**Disclaimer**

# Contents

# 1 Introduction

This explanatory provides additional information to MACsec and MKA of the AUTOSAR Standard.

## 1.1 Objectives

The objective of this document is to provide additional information and description of the MACsec and MKA protocols with the focus in AUTOSAR Adaptive Platform.

## 1.2 Scope

This document provides guidelines for MACsec integration in the AUTOSAR Adaptive Platform.

# 2 Definition of terms and acronyms

The glossary below includes acronyms and abbreviations relevant to the MKA module that are not included in the [1, AUTOSAR glossary].

## 2.1 Acronyms and abbreviations

| Abbreviation / Acronym: | Description: |
|---|---|
| AN | Association Number |
| CA | Secure Connectivity Association |
| CAK | Secure Connectivity Association Key |
| CKN | Connectivity Association Key Name |
| DA | Destination Address |
| EAP | Extensible Authentication Protocol |
| 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 |
| PSK | Pre-shared Key |
| 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 |
| TLV | Tag-Length-Value |

**Table 2.1: Acronyms and abbreviations used in the scope of this Document**

# 3 Related Documentation

## 3.1 Input documents & related standards and norms

MACsec Requirements Specification [2, RS MACsec] which is also valid for MKA.

[1] Glossary
AUTOSAR_FO_TR_Glossary

[2] Requirements on MACsec
AUTOSAR_FO_RS_MACsec

[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] Specification of Manifest
AUTOSAR_AP_TPS_ManifestSpecification

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

# 4 The basics of MACsec Protocol

## 4.1 MACsec protocol - network security standard

MACsec is a network security standard that operates at the Media Access Control (MAC) layer (Layer 2) and defines connectionless data confidentiality and integrity for media access independent protocols. MACsec stands for Media Access Control Security and it is defined and specified on the IEEE 802.1AE standard ([3, IEEE-802.1AE-2018]). It is a point-to-point (P2P) protection mechanism, which provides secure communication for Ethernet Networks, specifically protects communication channels within the vehicle network.

MACsec provides:

- Security solutions on the lowest media independent layer (Layer 2 or MAC Layer).
- Integrity protection. The layer 2 payload and MAC addresses of each frame are integrity protected.
- Confidentiality. Whenever configured, the layer 2 payload of each frame on the wire is encrypted.
- Advantages of using MACsec:
  - Confidentiality.
  - Flexibility.
  - Network intelligence.
  - Scalability.
  - Performance of the communication peer which includes MACsec protection is better than with other security protocols.
- Ensures data integrity, data origin authentication and the option of encryption mechanisms.
- Complements other existing security protocols in the upper layers (IPsec, TLS, SSH, . . .).
- Protecting P2P communication with MACsec, provides protection with lesser number of Secure Associations (SA).
- Hardware based MACsec protection supports high bandwidth links (making it more scalable) and also off loads a lot of work from the CPU.

Additionally to the MACsec standard ([3, IEEE-802.1AE-2018]), the MACsec Key Agreement Protocol (MKA) ([4, IEEE-802.1X-2020]) is required for the peer authentication, the key exchange and the establishment of the Secure Associations (SA).

MACsec protected frame consists of:

- MAC Security Tag (SecTAG) → Layer 2 header to identify the MACsec relevant information for the receiver and sender.
- Security Payload → Payload which is confidentiality protected with MACsec. (In case confidentiality is configured).
- ICV → Integrity Check Value for the payload including Layer 2 protocols.

MACsec supports three modes of operation:

- Integrity without confidentiality.
- Integrity with confidentiality without offset.
- Integrity with confidentiality with offset.

The following drawing shows an Ethernet frame including the MACsec protocol header:

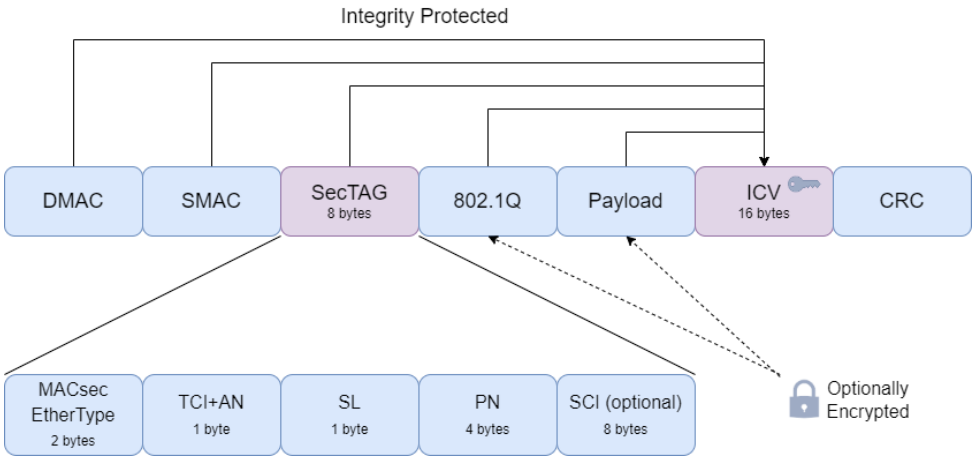


**Figure 4.1: Ethernet Frame including MACsec integrity and optionally confidentiality protection.**

As mentioned before, the MACsec protection is Point to Point (P2P), which requires independent secure channels between pairs of ports. For example, if between two peers, there is a switch, two different Secure Channels must be established. One between the Peer1 and the Switch, using the corresponding port (Port1), and a second one between the Switch, using the corresponding port (Port2), and the Peer2, as it is shown in the following figure.

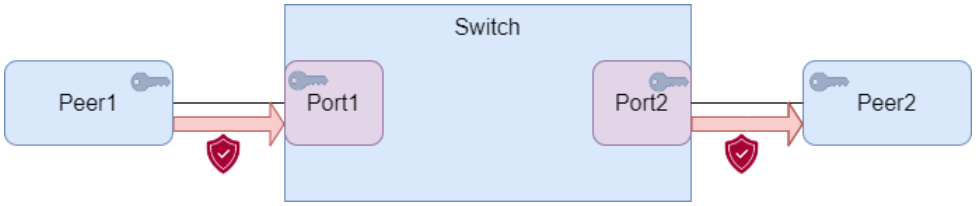


**Figure 4.2: MACsec communication between Peer1 and Peer2, with a switch in between.**

## 4.2 MACsec Key Agreement protocol (MKA)

The purpose of the MACsec Key Agreement (MKA) protocol is to provide a mechanism to discover MACsec peers and negotiate the security keys required to secure the link. There are two mechanisms defined within the 802.1X standard for the generation of key material for the use with MKA:

- Pre-shared Keys (PSK).
- The master session key which is a product of a successful Extensible Authentication Protocol (EAP) authentication. (More information on the [4, IEEE-802.1X-2020])

The current MACsec implementation guidelines rely on PSK, due to the much better performance in start-up times. That means the CAK, and its respective CKN, shall be pre-installed on the communication participants on advance.

The following drawing shows the corresponding sequence related to the MKA protocol:

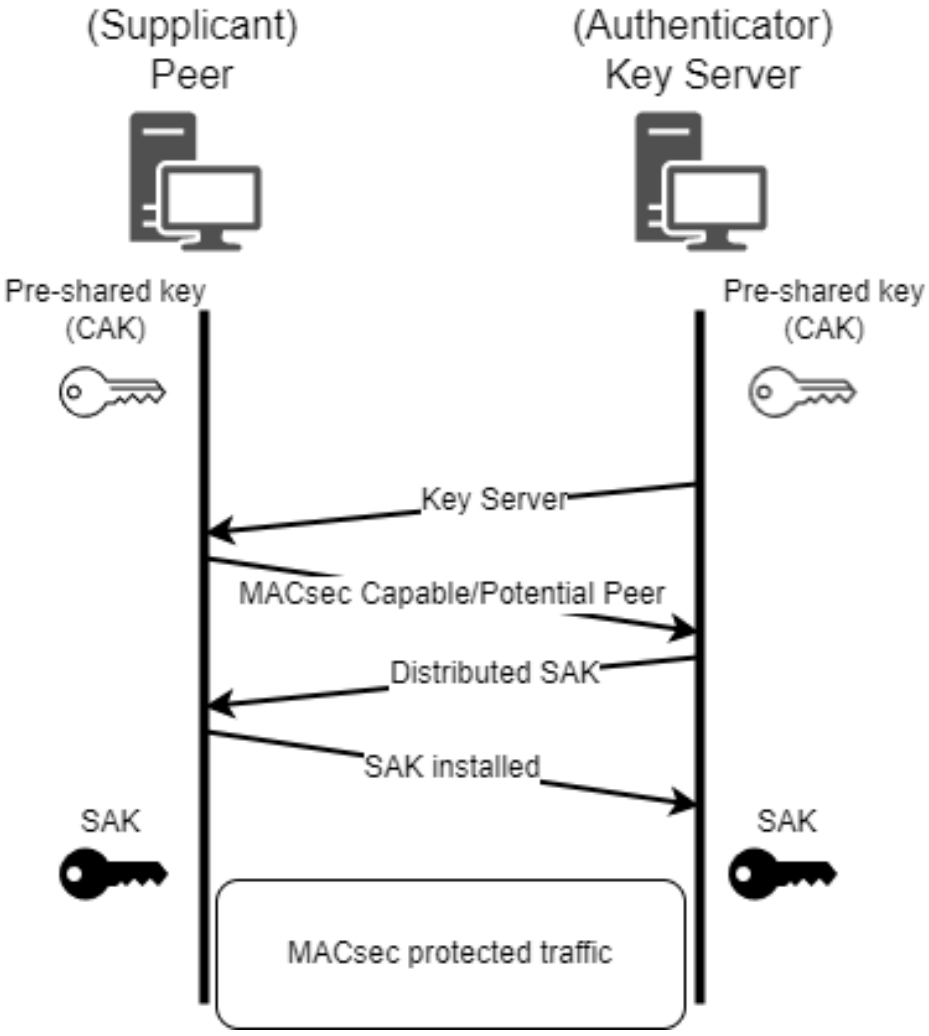


**Figure 4.3: MACsec Key Agreement sequence with pre-shared key.**

The participants present in the MKA communication, according to [4, IEEE-802.1X-2020], are:

- Supplicant, also known as client.
- Authenticator.
- Authentication Server.

In general, for automotive applications the Authenticator and the Authentication Server are preferred to be implemented in the same controller, named Key Server, and with the following advantages associated:

- Avoids extra communication with an onboard/internet external server.
- The delay introduced by the Authentication Server and the Authenticator communications is eliminated.

The MKA sequence is as follows:

- Key Server: the Authenticator node takes the so-called Key Server role announcing its MACsec capabilities and the information needed to take part in the communication.
- MACsec Capable/Potential Peer List: other Nodes receiving the packets sent by the Key Server, will join the MKA process if they belong to the same Connectivity Association (CA). These nodes will take the Supplicant role in the MKA communication and will respond with their MACsec Capabilities and the information needed to identify them.
- Live Peer List: Authenticator and Supplicant include each other's information on this list to communicate the proper authentication of the other communication partner.
- Distributed SAK: the Key Server distributes a new session key for MACsec (SAK) encrypted and integrity protected using the KEK and ICK derived from the CAK respectively.
- SAK installed: Both participants acknowledge the proper installation of the new key SAK for transmission and reception. From this moment on, MACsec is ready to use.

# 5 Objective of MACsec

The objective of MACsec protocol implementation in AUTOSAR Adaptive Platform is providing secure communication links in the in-vehicle Ethernet network. Implementing MACsec in AUTOSAR Adaptive Platform provides options for securing communication between nodes with confidentiality, integrity or both guaranteed.

# 6 Primary recommendations

## 6.1 Prerequisites

MACsec is a security protocol in Layer 2, which means, it is fully dependent on Ethernet functionality, but also the system shall include a MKA Daemon for the establishment of the Secure Channels between nodes.

## 6.2 Implementation of MACsec in AUTOSAR AP stack

The AUTOSAR's Adaptive Platform does not specify any operating system for an Electronic Control Unit (ECU) and as of that, implementing state-of-the-art MACsec functionality along with best practices, is a shared responsability of the stack vendor and the stack integrator.

This goal can be achieved without engaging any higher network stack level, i.e. communication channel established with MACsec would be fully transparent for AUTOSAR Adaptive Platform Communication Management functional cluster, thus for Adaptive Applications as well.

The following picture outlines the design of the AUTOSAR Adaptive stack. The only part of the functionality, which is included in the Specification of Manifest [5, AUTOSAR_AP_TPS_ManifestSpecificacion], is the "MKA config". This is only an example, based on Linux architecture and might require some modifications for other operating systems.

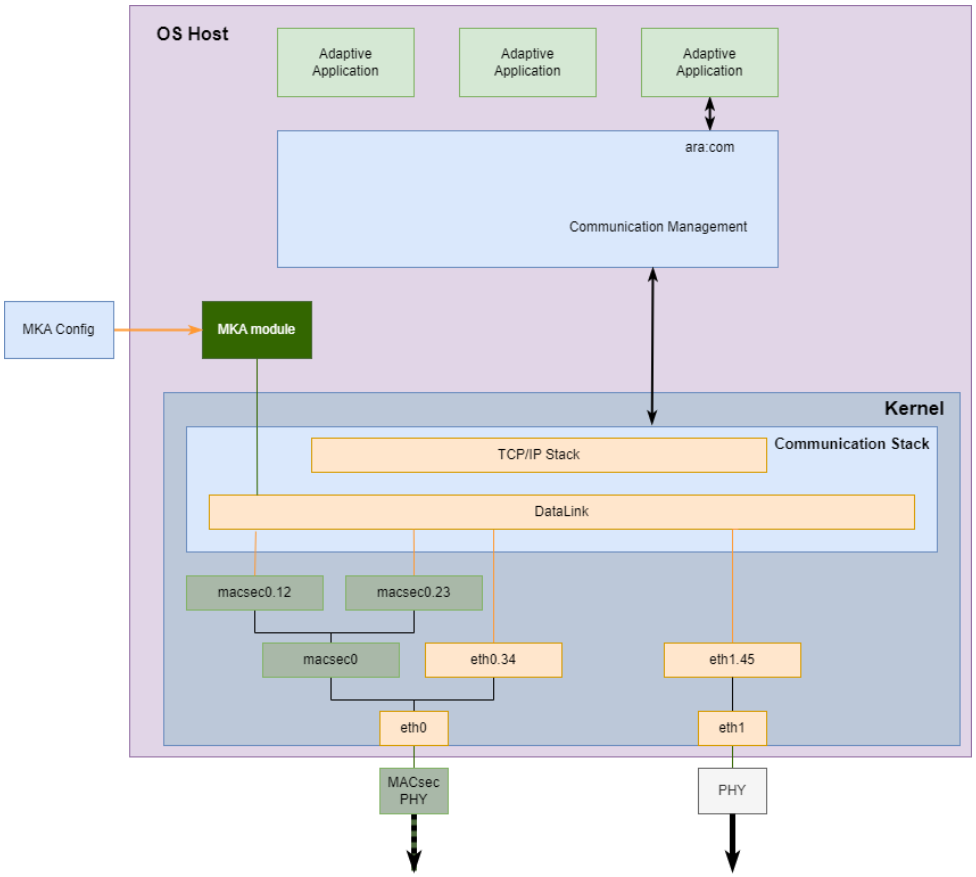


**Figure 6.1: Communication with MKA Module in AUTOSAR Adaptive Platform.**

If a Host has the architecture of the previous drawing, the following actions happen until the Host sends the first MACsec protected frame.

- Kernel startup: the physical interfaces are detected and the driver is initialized.
- Initialization of the network configuration: configuration of the Phy/Switch (Link Speed, MACsec enabling, ...), setup of VLANs (Virtual VLAN interfaces are created) and configuration of MACsec bypass rules in the Phy/Switch (Bypassed VLANs, Ethertype 0x88E5, MKA). At this point, the interfaces which does not use MACsec (eth0, eth0.34, eth1 and eth1.45 on the figure) have already signaled a link up. The rest signal a link down.
- Launch MKA Daemon: generate virtual MACsec interfaces as defined in the configuration files:
  - eth0 $\rightarrow$ macsec0 (down)
  - macsec0.12 (down) (virtual VLAN interface over macsec0)
  - macsec0.23 (down) (virtual VLAN interface over macsec0)
- Launch of non-MACsec stacks/Daemons (Communication Management, Adaptive Applications, ...). From this moment, non-protected frames can be sent through the unprotected adapters.

- MKA Daemon starts MKA sequence: start MKA exchange sequence and install SAKs in the MACsec entity (Phy, switch or software based MACsec).

Once this process has been finished the MACsec interfaces will indicate link up, which means MACsec protected frames can be sent.

## 6.3 Operating System's kernel using MKA Module

As mentioned above, MACsec requires the usage of the OS Ethernet components, usually located in the kernel area. MKA Module shall be called from the different modules of the Kernel, related to the Ethernet communication, for the implementation of the MKA and MACsec functionalities.

## 6.4 MKA Module

In order to make MACsec operative, a MACsec Key Exchange Agreement (MKA) module is needed. Typically, it would not be a part of the kernel space and require a separated implementation and integration. For the Host OS, MKA as defined in [4, IEEE-802.1X-2020] shall be implemented. For the MKA Daemon a configuration file is needed, to set the bypass rules, the MACsec ports, the list of CKNs, . . ..

MKA module needs to be initialized during the OS boot time in order to assure that all necessary security associations are established before the node starts communication through the MACsec protected Ethernet channels.

# 7 Detailed features description for MACsec implementation

While integrating MACsec in AUTOSAR Adaptive Platform, the following features shall be included in the implementation. That ensures compatibility and superior security posture. The [2, RS MACsec] document shall be consulted for detailed requirements.

- MACsec is supported based on the following standards:
  - MACsec standard (Media Access Control Security) → [3, IEEE-802.1AE-2018]
  - MACsec Key Agreement protocol (MKA) for the exchange of secret keys used in MACsec → [4, IEEE-802.1X-2020]
  - AUTOSAR requirements on MACsec → [2, RS MACsec]
- Following common features are fulfilled:
  - Using MACsec on external communication links.
  - Configure which Ethernet ports use MACsec.
  - The implementation of MKA provides an option to control and monitor the MACsec state of the interfaces. Activation, deactivation and readout of MACsec status on a network interface.
  - The Adaptive AUTOSAR Platform's Operating System provides mechanisms to configure the MACsec related resources.
  - Configuration of unprotected traffic is provided.
  - Monitoring of the MACsec channels status and statistics.
- The MACsec implementation supports the following features regarding the MACsec protocol:
  - Support of integrity and confidentiality protection.
  - MAC Security TAG (SecTAG).
  - MACsec EtherType (0x88E5).
  - Support of extended packet numbering (XPN).
  - Secure Channel Identifier (SCI).
  - Secure Data.
  - Integrity Check Value (ICV).
  - In SW solution: Protect and validation functions.
- The MACsec implementation is integrated on the Host OS.

- The MACsec implementation supports the following features regarding the MKA protocol:
  - Support of MKA packets.
  - Pre-shared key support.
  - Key selection based on connectivity association key name (CKN).
- The MACsec implementation supports the following features regarding cryptography:
  - Support Key Encryption Key (KEK).
  - Support Integrity Check Value Key (ICK).
  - Support of Key Derivation Function (KDF). KDF uses the AES Cipher in CMAC mode ([6, IETF RFC 4493]).
  - The MACsec entity shall support these algorithms as Cypher Suites:
    - GCM-AES-128
    - GCM-AES-256
    - GCM-AES-XPN-128
    - GCM-AES-XPN-256
  - Validation and generation functions for ICVs.
- The MACsec implementation assumes two participants per link.
- The MKA implementation supports retry of the MKA sequence.
- The MKA implementation supports re-key of SAKs as specified in [IEEE-802.1X-2020]{IEEE-8021X-2020} and additionally in any of the following conditions:
  - After a configurable time span.
  - The packet number space of one direction (sending or receiving) exceeds:
    - 0xC000 0000 for 32-bit PNs.
    - 0xC000 0000 0000 0000 for 64-bit PNs (XPN mode).
- IDSM has to be linked with MACsec Security Events (FO_RS_MACsec_00009) to collect the needed information for diagnostic/logging purpose.

# 8 Further guidance

## 8.1 Backward compatibility

Electronic Control Units with MACsec support shall allow integration into vehicles, in which their communication partners do not support MACsec.

Configuration options for MACsec communication for specific peers shall be available.

## 8.2 MACsec bypass rules

The ECU shall support that certain Ethernet Types or VLAN IDs can be bypassed, that means for the corresponding communication there is no MACsec protection, neither integrity nor confidentiality.

# 9 Supplementary information

The above mentioned requirements should not be regarded as exhaustive, and the final implementation does not need to be restricted to them.

In particular, documentation specific to software packets picked out for integration with the operating system stack should be taken into consideration.