Document Title	Explanation of IPsec Implementation Guidelines
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	930

Document Status	published
Part of AUTOSAR Standard	Adaptive Platform
Part of Standard Release	R19-11

Document Change History			
Date	**Release**	**Changed by**	**Description**
2019-11-28	R19-11	AUTOSAR Release Management	• No content changes • Changed Document Status from Final to published
2019-03-29	19-03	AUTOSAR Release Management	• No content changes
2018-10-31	18-10	AUTOSAR Release Management	• Initial release

Disclaimer

Table of Contents

1 Introduction

1.1 Scope of this document

This document provides guidelines for IPsec implementation in the AUTOSAR Adaptive Platform.

1.2 Relation to other standards

This document is relevant to AUTOSAR Adaptive Platform only.

2 The Basics of IPsec Protocol

2.1 IPsec protocol - network security standard

IPsec is a network layer protocol suite that secures network connections by encrypting or authenticating IP packets. It constitutes a part of IP protocol suite.

IPsec consists of three elementary components:

- Internet Key Exchange - most widely used module for key management
- Authentication Header - (IP protocol 51) for integrity
- Encapsulating Security Payload - (IP protocol 50) for integrity and confidentiality

It is an open network standard, maintained by IETF since 1995 and commonly used in network equipment as well as server and desktop operating systems.

The IPsec can be implemented in the IP stack of an operating system, which requires modification of the source code. This method of implementation is done for many host and security gateway operating systems.

IPsec works in two basic modes of operation:

- Transport mode
- Tunnel mode

The following drawings explain packet structure of Authentication Header and Encapsulating Security Payload.

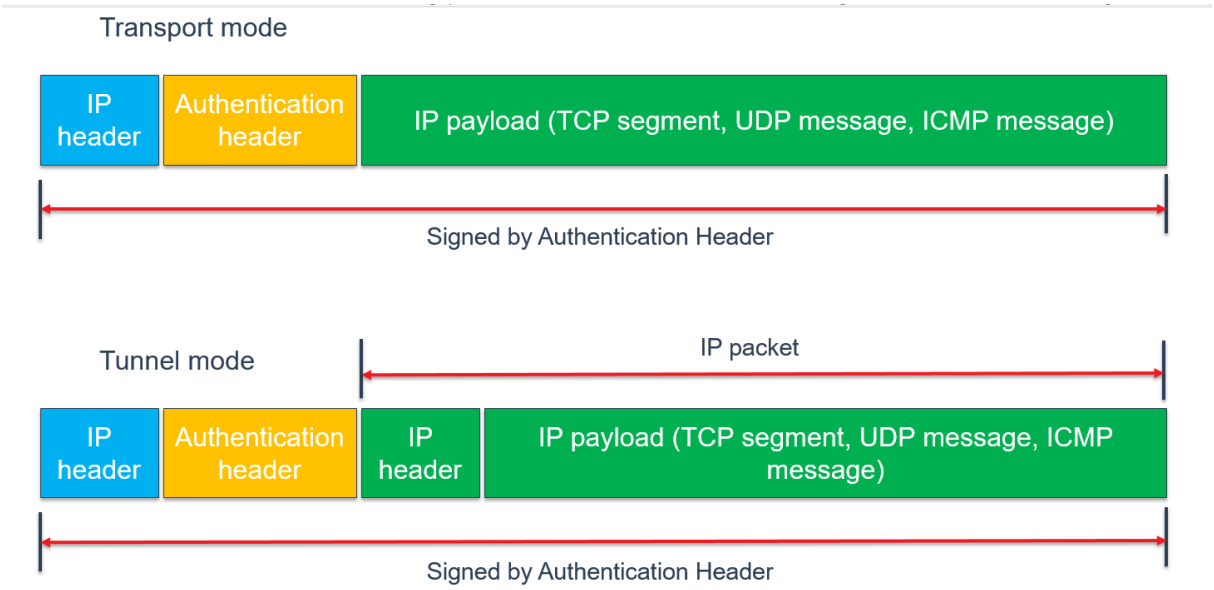

Figure 2.1: Authentication Header (AH) frame

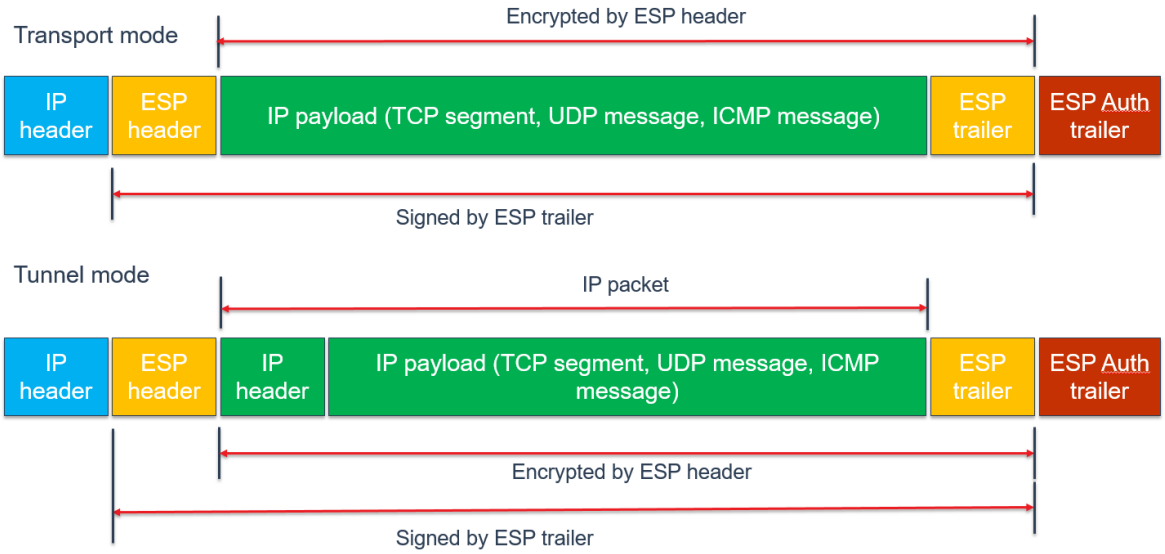

Figure 2.2: Encapsulating Security Payload (ESP) frame

2.2 Internet Key Exchange operation

In order to create session keys necessary for the network traffic protection IKE starts key exchange and stores Security Associations. A Security Association (SA) is the formation of shared security elements between two network nodes in order to support secure communication. It may include attributes such as: cryptographic algorithm and mode, traffic encryption key, and parameters for the network data to be passed over the connection. They are usually stored in Security Associations Database.

Usually, a Security Association consists of at least the following parameters:

- Destination IP address
- Security Parameter Index (SPI)
- IPsec protocol identifier (AH / ESP)
- Mode (transport / tunnel)
- Key and algorithms used
- Lifetime

The following drawing explains the meaning of IKE module, security associations and security policies databases for securing IPsec network communication.

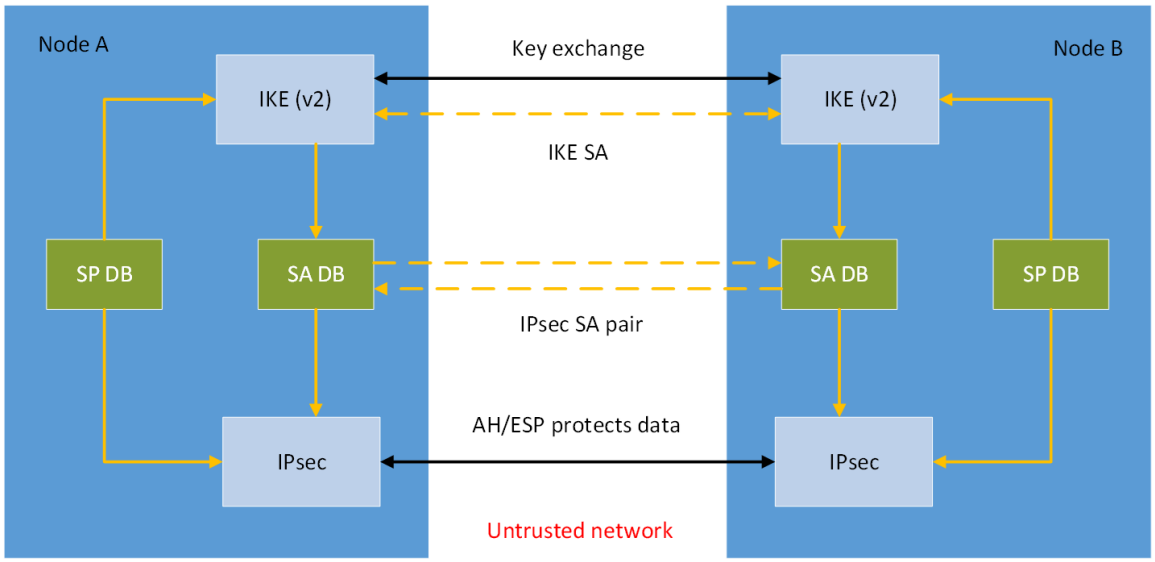

Figure 2.3: SA creation with IKE for network traffic protection

3 Objective

The objective of IPsec protocol implementation in AUTOSAR Adaptive Platform is providing secure communication channels in the in-vehicle IP network.

Implementing IPsec in AUTOSAR Adaptive Platform would provide options for securing communication between network nodes with confidentiality, integrity or both guaranteed.

IPsec, as a standard network security protocol provides means for secure communication, while supporting multi-vendor stack interoperability.

4 Primary recommendations

4.1 Prerequisites

As IPsec is a subset of IP protocol suite and is fully dependent on IP stack functionality, a fully useful IP stack enables IP network packet flow, necessary for IPsec protocol service.

4.2 Implementation of IPsec in AUTOSAR AP stack

Adaptive Platform does not specify any operating system for an Electronic Control Unit (ECU) and as of that, implementing state-of-the-art IPsec functionality along with best practices, it is the stack vendor responsibility.

This goal can be achieved without engaging any higher network stack level, i.e. communication channel established with IPsec 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 functionality of the stack, presented below Communication Management there, is defined in AUTOSAR Adaptive Platform documentation only in the Specification of Manifest [17], what is represented as 'IKE config' and 'IPsec config' here.

This is only an example, based on Linux architecture and might require some modifications for other operating systems.

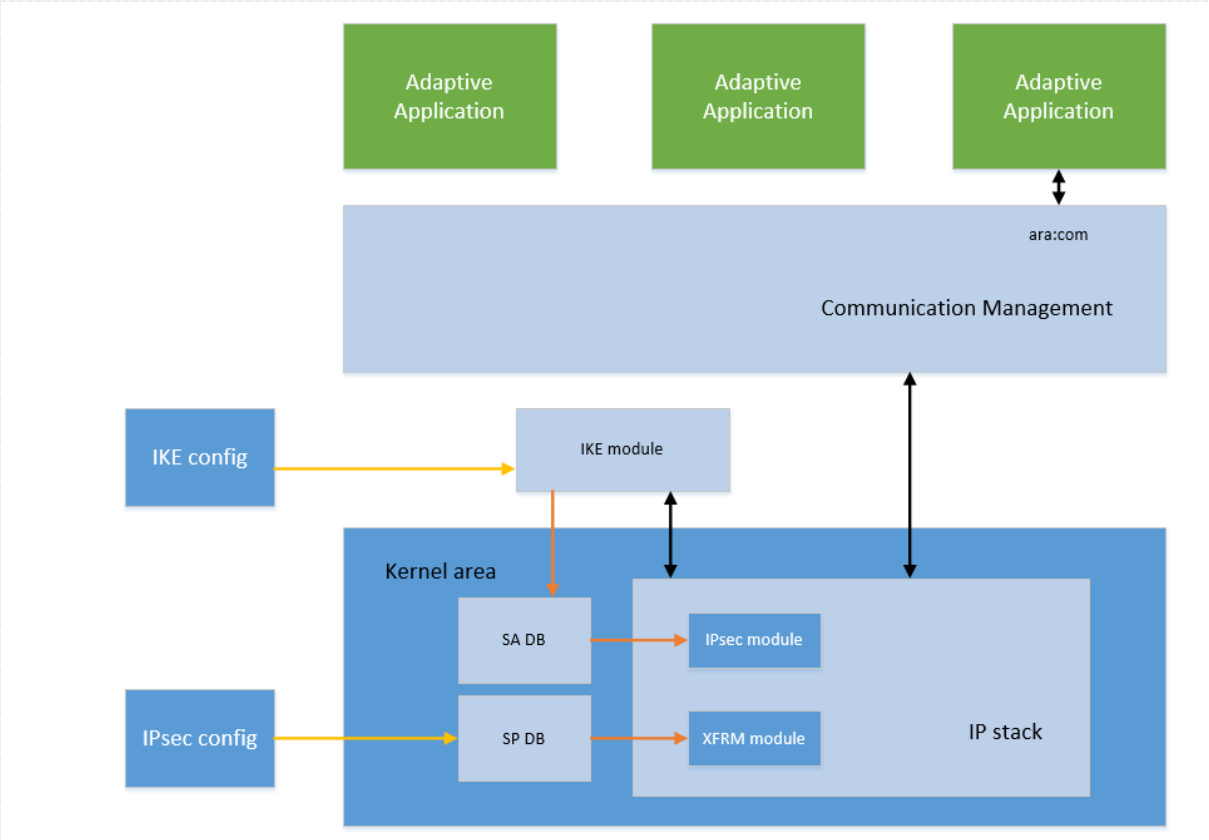

Figure 4.1: Communication with IPsec in AUTOSAR Adaptive Platform

4.3 Operating System kernel with an IP stack

As mentioned above, IPsec requires OS usage of an IP stack, usually located in the kernel area. Being just a subset of the IP protocol suite, and a part of the IP stack in the end, IPsec would need to be integrated with the bare IP stack. That would be routinely obtained with compiling OS kernel along with IP stack and IPsec modules.

4.4 Kernel IPsec module

Most of current operating systems offer modern IP stack modules, extensible with IPsec functionality. They should be applied along with filtering modules (like e.g. the XFRM Framework in Linux), allowing packet management according to IPsec rules, as described in Specification of Manifest [17].

IPconfig part defined in Specification of Manifest would be typically represented as security policies, forming security policies database, but it depends on implementation in the end.

4.5 IKE module

In order to make IPsec operative an Internet Key Exchange (IKE) module is needed. Typically, it would not be a part of the kernel space and require separated integration.

For AUTOSAR Adaptive Platform IKE version 2 should be used. IKEv2 provides modern security options and is eventually easier to implement.

IKE config would usually stand for a configuration file.

IKE module needs to be initialised during boot process in order to make sure all necessary security associations would be ready before the node starts communication.

5 Detailed requirements for IPsec implementation

While integrating IPsec in AUTOSAR Adaptive Platform, the following requirements should be met. That would ensure compatibility and superior security posture.

5.1 IPsec shall be implemented based on the following standards:

- "Security Architecture for the Internet Protocol" [2]
- "Authentication Header (AH)" [3]
- "Encapsulating Security Payload (ESP)" [4]

5.2 The IPsec implementation shall support Extended Sequence Number [5]

5.3 The implementation shall support these algorithms for AH and use them in this preferences order (highest priority first):

- AUTH_AES_GMAC: AES Galois Message Authentication Code (GMAC) [6]
- AUTH_AES_CMAC_96: AES Cipher-based Message Authentication Code (CMAC) [7]

5.4 The following algorithms for ESP shall be supported in this priority:

- AES-GCM with 16 octet ICV [8]
- ENCR_AES_CCM_16 [9]

5.5 The IPsec implementation shall support at least Suite-B-GMAC-128 from [10] for both ESP and AH

5.6 Internet Key Exchange Protocol Version 2 (IKEv2) shall be supported [11]

5.7 The IKEv2 implementation shall support authentication based on X.509v3 Certificates with digital signatures [12]

5.8 IKEv2 shall gracefully shutdown by sending DELETE_SAs on closure and rebuilding them on startup

5.9 IKEv2 shall use Dead Peer Detection

5.10 Configuration shall define the rekey interval for SA and child SA

5.11 The implementation shall support a seamless handover between exchanged keys

5.12 IPsec implementation shall use the Transport Mode

5.13 IPsec Tunnel Mode is currently not supported

5.14 The following ports shall be not protected by IPsec:

- 500/UDP: IKEv2 packets
- 4500/UDP: IKEv2 packets
- 6801/TCP: Diagnostics

6 Further guidance

6.1 Multicast communication

Multicast communication secured with IPsec is currently not planned for AUTOSAR Adaptive Platform, what simplifies key management and reduces the risk of a key disclosure.

These benefits for smaller networks, like in-vehicle network, would usually prevail.

6.2 Retry for key update

If the peer ECU is not available when keys shall be updated, the ECU retries, whether the peer ECU is available again. That way security association can be obtained despite a temporary node unavailability.

6.3 Backward Compatibility

Electronic Control Units with IPsec support shall allow integration into vehicles, in which their communication partners do not support IPsec. Configuration options for either IP or IPsec communication for specific peers shall be available.

6.4 Filtering with IPsec rules

The ECU shall support that certain application sockets - IP address, protocol, and port number - can only be connected using IPsec.

6.5 Patch Management

It is highly recommended to check, if there is an update available for libraries integrated in the IPsec kernel module or IKE module, and apply them whenever possible.

6.6 Security Functions Development

When there is a new cryptographic function available, like e.g. new encryption algorithm, it would make sense to introduce it. It would work reasonable, however, only when performed based on approved RFC documents.

7 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.

8 Related documentation

[1] AUTOSAR Specifications in general

[2] RFC 4301

[3] RFC 4302

[4] RFC 4303

[5] RFC 4304

[6] RFC 4543

[7] RFC 4494

[8] RFC 4106

[9] RFC 4309

[10] RFC 6379

[11] RFC 7296

[12] RFC 7427

[13] RFC 3602

[14] RFC 4868

[15] RFC 5903

[16] Specification of Manifest

9 Acronyms and Abbreviations

The glossary below includes acronyms and abbreviations relevant to the explanation of IPsec implementation in AUTOSAR Adaptive Platform.

Abbreviation / Acronym:	Description:
AH	Autenticating Header protocol
DB	Database
ECU	Electronic Control Unit
ESP	Encapsulating Security Payload protocol
IKE	Internet Key Exchange protocol
IP	Internet protocol
IPsec	Internet Protocol Security protocol
SA	Security Association