Document Title	Requirements on IPsec Protocol
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	970

Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R25-11

Document Change History			
Date	**Release**	**Changed by**	**Description**
2025-11-27	R25-11	AUTOSAR Release Management	• Editorial changes • Remove requirements tracing to RS_Main
2024-11-27	R24-11	AUTOSAR Release Management	• No content changes
2023-11-23	R23-11	AUTOSAR Release Management	• No content changes
2022-11-24	R22-11	AUTOSAR Release Management	• No content changes
2021-11-25	R21-11	AUTOSAR Release Management	• No content changes
2020-11-30	R20-11	AUTOSAR Release Management	• No content changes • Changed Document Status from Final to published
2019-11-28	R19-11	AUTOSAR Release Management	• Initial release

Disclaimer

This work (specification and/or software implementation) and the material contained in it, as released by AUTOSAR, is for the purpose of information only. AUTOSAR and the companies that have contributed to it shall not be liable for any use of the work.

The material contained in this work is protected by copyright and other types of intellectual property rights. The commercial exploitation of the material contained in this work requires a license to such intellectual property rights.

This work may be utilized or reproduced without any modification, in any form or by any means, for informational purposes only. For any other purpose, no part of the work may be utilized or reproduced, in any form or by any means, without permission in writing from the publisher.

The work has been developed for automotive applications only. It has neither been developed, nor tested for non-automotive applications.

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

Table of Contents

1 Scope of Document 4

2 Conventions to be used 5

3 Acronyms and abbreviations 6

4 Requirements Specification 7

4.1 Functional Overview 7
4.2 Functional Requirements 7

5 References 16

A Change history of AUTOSAR traceable items 17

A.1 Traceable item history of this document according to AUTOSAR Release R25-11 17
A.1.1 Added Requirements in R25-11 17
A.1.2 Changed Requirements in R25-11 17
A.1.3 Deleted Requirements in R25-11 17
A.2 Traceable item history of this document according to AUTOSAR Release R24-11 17
A.2.1 Added Requirements in R24-11 17
A.2.2 Changed Requirements in R24-11 17
A.2.3 Deleted Requirements in R24-11 17
A.3 Traceable item history of this document according to AUTOSAR Release R23-11 18
A.3.1 Added Requirements in R23-11 18
A.3.2 Changed Requirements in R23-11 18
A.3.3 Deleted Requirements in R23-11 18

1 Scope of Document

This document defines requirements of IPsec in the AUTOSAR Foundation. The motivation is to ensure interoperability of IPsec within Adaptive platforms and between Adaptive and Classic configurations.

2 Conventions to be used

The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078], see [1, Standardization Template].

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

3 Acronyms and abbreviations

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

Abbreviation / Acronym	Description
AH	Authentication Header
DB	Database
ESP	Encapsulating Security Payload
ICV	Integrity Check Value
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPsec	Internet Protocol Security
PAD	Peer Authorization Database
PKI	Public Key Infrastructure
PSK	Pre-Shared Keys
RAM	Random Access Memory
SA	Security Association
SAD	Security Association Database
SPD	Security Policy Database
TCP/IP	Transmission Control Protocol / Internet Protocol
V2X	Vehicle to everything

4 Requirements Specification

This chapter describes all requirements driving the work to define the IPsecProtocol.

4.1 Functional Overview

IPsec is a standard for authentication and encryption on the IP protocol layer 3. How it works in general and is intended to be used in AUTOSAR is described in the IPsec implementation explanatory [3].

In general, strongSwan [4] is used as reference. It is an open source implementation of IPsec. If there are any uncertainties about the IPsec protocol from the general RFCs describing it [5], [6], [7], [8] or the requirements defined in this document, the strongSwan implementation can be checked for clarification.

4.2 Functional Requirements

[RS_IPSEC_00001] IPsec shall be supported according to IETF RFC 4301 ⌈

Description:	IPsec shall be supported according to IETF RTF 4301. Limitation: all requirements related to tunnel mode are optional, e.g. section 5.1.2, 7.1 and 7.2
Rationale:	To enable secured communication over IP
Dependencies:	–
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4301 [5]

⌋

[RS_IPSEC_00002] The IP Authentication Header (AH) shall be supported according to IETF RFC 4302 ⌈

Description:	The IP Authentication Header (AH) shall be implemented in the TCP/IP stack as stated in IETF RFC 4302. Limitation: Section 3.1.2, related to tunnel mode, may or may not be implemented
Rationale:	To enable secured communication over IP
Dependencies:	[RS_IPSEC_00001]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4302 [6]

⌋

[RS_IPSEC_00003] IP Encapsulating Security Payload (ESP) shall be supported according to IETF RFC 4303

Status: DRAFT

⌈

Description:	The IP Encapsulating Security Payload (ESP) shall be implemented in the TCP/IP stack as stated in IETF RFC 4303. Limitation: Any section related to tunnel mode, may or may not be implemented, e.g. section 3.1.2
Rationale:	To enable secured communication over IP
Dependencies:	[RS_IPSEC_00001]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4303 [7]

⌋

[RS_IPSEC_00004] The Internet Key Exchange (IKEv2) Protocol shall be supported according to IETF RFC 7296 ⌈

Description:	The Internet Key Exchange (IKEv2) Protocol shall be implemented in the TCP/IP stack as stated in IETF RFC 7296. The old IKEv1 shall not be supported. Limitation: Support is limited to scenario 1.1.2 Endpoint-to-Endpoint Transport
Rationale:	To enable secured communication over IP
Dependencies:	[RS_IPSEC_00001]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 7296 [8]

⌋

[RS_IPSEC_00005] Extended sequence numbers (ESN) for AH and ESP shall be supported according to IETF RFC 4304 ⌈

Description:	Extended sequence numbers (ESN) for AH and ESP shall be supported according to IETF RFC 4304
Rationale:	To enable secured communication over IP
Dependencies:	[RS_IPSEC_00002], [RS_IPSEC_00003]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4304 [9]

⌋

[RS_IPSEC_00006] If encryption is used in IPsec, authentication shall be used as well

Status: DRAFT

⌈

Description:	If encryption is used in IPsec, authentication shall be used as well according to IETF RFC 8221 section 4
Rationale:	Unauthenticated encryption is insecure
Dependencies:	[RS_IPSEC_00001]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 8221 [10]

⌋

[RS_IPSEC_00007] Pre-shared keys (PSK) may be used in combination with IKEv2 ⌈

Description:	Pre-shared keys (PSK) may be used in combination with IKEv2
Rationale:	Makes slightly faster startup possible, compared to using digital signatures, but at the cost of additional key management
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	–

⌋

[RS_IPSEC_00008] Pre-shared keys (PSK) shall not be used for directly setting up IPsec security associations (SAs) ⌈

Description:	Pre-shared keys (PSK) shall not be used for directly setting up IPsec security associations (SAs). See IETF RFC 8221 section 3
Rationale:	Using PSKs to set up SAs directly would break many security features like perfect forward secrecy and make replay attacks easier
Dependencies:	[RS_IPSEC_00001]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 8221 [10]

⌋

[RS_IPSEC_00009] Counter mode encryption algorithms shall not be used in combination with pre-shared keys when setting up SAs directly ⌈

Description:	Counter mode encryption algorithms, e.g. $ENCR_AES_CCM_16$ and $ENCR_AES_GCM_16$, shall not be used in combination with pre-shared keys when setting up SAs directly according to IETF RFC 8221 section 3

▽

△

Rationale:	Counter mode algorithms break even more security assumptions than [RS_IPSEC_00008]
Dependencies:	[RS_IPSEC_00001]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 8221 [10]

⌋

[RS_IPSEC_00010] IKEv2 shall support periodic reauthentication and rekeying ⌈

Description:	IKEv2 shall support periodic reauthentication and rekeying of the IKEv2 communication partners according to IETF RFC 7296 section 1.3.2 and 1.3.3
Rationale:	Considered good security practice, limits usefulness of stolen keys to shorter time periods
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 7296 [8]

⌋

[RS_IPSEC_00011] IKEv2 shall support a seamless handover of exchanged keys ⌈

Description:	IKEv2 shall support a seamless handover of exchanged keys according to IETF RFC 7296 section 2.8. That means, during rekeying or reauthentication it should create new overlapping SAs first before it deletes the old SAs ("make before break"), so that the service is not interrupted. IETF RFC 4478 may be supported.
Rationale:	To avoid service interruption during rekeying phases
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 7296 [8], IETF RFC 4478 [11]

⌋

[RS_IPSEC_00012] IKEv2 shall gracefully delete all SAs on shutdown and rebuild the deleted SAs immediately after the next startup ⌈

Description:	IKEv2 shall gracefully delete all SAs on shutdown according to IETF RFC 7296 section 1.4.1 and rebuild the deleted SAs immediately after the next startup.
Rationale:	To keep the stateless properties of IPsec while minimizing service interruptions
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 7296 [8]

⌋

[RS_IPSEC_00013] IKEv2 shall support dead peer detection ⌈

Description:	IKEv2 shall use dead peer detection according to IETF RFC 7296 section 2.4. IETF RFC 3706 may be supported.
Rationale:	Bandwidth management, to avoid sending data to dead peers
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 7296 [8], IETF RFC 3706 [12]

⌋

[RS_IPSEC_00014] IKEv2 shall support authentication based on X.509v3 certificates with digital signatures ⌈

Description:	IKEv2 shall support authentication based on X.509v3 certificates with digital signatures according to IETF RFC 7427.
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 7427 [13]

⌋

[RS_IPSEC_00015] IPsec shall support the following authentication algorithm: AES Galois Message Authentication Code with 256 bit keys ⌈

Description:	IPsec shall support the following authentication algorithm: AES Galois Message Authentication Code ($AUTH_AES_256_GMAC$) with 256 bit keys according to IETF RFC 4543
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00002], [RS_IPSEC_00003], [RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4543 [14]

⌋

[RS_IPSEC_00016] IPsec shall support the following authentication algorithm: AES Cipher-based Message Authentication Code with 128 bit keys ⌈

Description:	IPsec shall support the following authentication algorithm: AES Cipher-based Message Authentication Code ($AUTH_AES_CMAC_96$) with 128 bit keys according to IETF RFC 4494
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00002], [RS_IPSEC_00003], [RS_IPSEC_00004]
Use Case:	In-vehicle secure communication

▽

△

Supporting Material:	IETF RFC 4494 [15]

⌋

[RS_IPSEC_00017] IPsec shall support the following encryption algorithm: AES Galois/Counter Mode with 256 bit keys and an integrity check value (ICV) of 16 octets

Status: DRAFT

⌈

Description:	IPsec shall support the following encryption algorithm: AES Galois/Counter Mode ($ENCR_AES_GCM_16$) with 256 bit keys and an integrity check value (ICV) of 16 octets according to IETF RFC 4106
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00003], [RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4106 [16]

⌋

[RS_IPSEC_00018] IPsec shall support the following encryption algorithm: AES in Counter with CBC-Mac Mode with 256 bit keys and an integrity check value (ICV) of 16 octets

Status: DRAFT

⌈

Description:	IPsec shall support the following encryption algorithm: AES in Counter with CBC-Mac Mode ($ENCR_AES_CCM_16$) with 256 bit keys and an integrity check value (ICV) of 16 octets according to IETF RFC 4309
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00003], [RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4309 [17]

⌋

[RS_IPSEC_00019] IPsec and IKEv2 shall support the following cryptographic suite: Suite-B-GMAC-256. If NULL encryption is used, authentication shall be provided by AH instead of ESP ⌈

Description:	IPsec and IKEv2 shall support the following cryptographic suite: Suite-B-GMAC-256 according to IETF RFC 6379 section 3.4. If NULL encryption is used, authentication shall be provided by AH instead of ESP

▽

△

Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00003], [RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 6379 [18]

⌋

[RS_IPSEC_00020] IPsec and IKEv2 shall support the following cryptographic suite: Suite-B-GMAC-128. If NULL encryption is used, authentication shall be provided by AH instead of ESP ⌈

Description:	IPsec and IKEv2 shall support the following cryptographic suite: Suite-B-GMAC-128 according to IETF RFC 6379 section 3.3. If NULL encryption is used, authentication shall be provided by AH instead of ESP
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00003], [RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 6379 [18]

⌋

[RS_IPSEC_00021] All algorithms which are classified as "MUST" in IETF RFC 8247 shall be supported by IKEv2

Status: DRAFT

⌈

Description:	All algorithms which are classified as "MUST" in IETF RFC 8247 shall be supported by IKEv2. Algorithms classified as "MUST-" or lower may be supported.
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 8247 [19]

⌋

[RS_IPSEC_00022] IPsec's Security Policy Database (SPD) shall be configurable for IPs, IP ranges, protocols, ports and port ranges ⌈

Description:	IPsec's Security Policy Database (SPD) shall be configurable for IPs, IP ranges, protocols, ports and port ranges according to IETF RFC 4301 section 4.4.1.1.
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00001]

▽

△

Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4301 [5]

⌋

[RS_IPSEC_00023] IPsec's Security Policy Database (SPD) default behavior shall be BYPASS ⌈

Description:	IPsec's Security Policy Database (SPD) default behaviour shall be BYPASS, that is not to use IPsec. That means, for any TCP/IP endpoints, for which no configuration can be found in the SPD, the traffic shall pass through without IPsec protections.
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00001]
Use Case:	In-vehicle secure communication
Supporting Material:	–

⌋

[RS_IPSEC_00024] IPsec shall not be used to protect the following ports: 500/UDP and 4500/UDP: used by IKEv2 ⌈

Description:	IPsec shall not be used to protect the following ports: 500/UDP and 4500/UDP: used by IKEv2
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00001]
Use Case:	In-vehicle secure communication
Supporting Material:	–

⌋

[RS_IPSEC_00025] IPsec's Peer Authorization Database (PAD) shall be configurable for use with X.509v3 ⌈

Description:	IPsec's Peer Authorization Database (PAD) shall be configurable for use with X.509v3 certificates according to IETF RFC 4301 section 4.4.3.
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00001], [RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	IETF RFC 4301 [5]

⌋

[RS_IPSEC_00026] IPsec's Peer Authorization Database (PAD) shall be configurable for use with pre-shared keys (PSK) ⌈

Description:	IPsec's Peer Authorization Database (PAD) shall be configurable for use with pre-shared keys (PSK)
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	

⌋

[RS_IPSEC_00027] It shall be possible to define the priority order of the algorithms used by IKEv2 during the IKE_INIT negotiations ⌈

Description:	IKEv2 will be used to negotiate which algorithms are used during the IKEv2 INIT phase. It shall be possible, but not required, to set a priority ordering of the algorithms which can be used.
Rationale:	Support industry security standard
Dependencies:	[RS_IPSEC_00004]
Use Case:	In-vehicle secure communication
Supporting Material:	

⌋

5 References

[1] Standardization Template
AUTOSAR_FO_TPS_StandardizationTemplate

[2] Glossary
AUTOSAR_FO_TR_Glossary

[3] Explanation of IPsec Implementation Guidelines
AUTOSAR_AP_EXP_IPsecImplementationGuidelines

[4] strongSwan website
https://www.strongswan.org

[5] RFC 4301, Security Architecture for the Internet Protocol

[6] RFC 4302, IP Authentication Header

[7] RFC 4303, IP Encapsulating Security Payload (ESP)

[8] RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2)

[9] RFC 4304, Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association

[10] RFC 8221, Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)

[11] RFC 4478, Repeated Authentication in Internet Key Exchange (IKEv2) Protocol

[12] RFC 3706, A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

[13] RFC 7427, Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)

[14] RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH

[15] RFC 4494, The AES-CMAC-96 Algorithm and Its Use with IPsec

[16] RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)

[17] RFC 4309, Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)

[18] RFC 6379, Suite B Cryptographic Suites for IPsec

[19] RFC 8247, Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)

A Change history of AUTOSAR traceable items

Please note that the lists in this chapter also include traceable items that have been removed from the specification in a later version. These items do not appear as hyperlinks in the document.

A.1 Traceable item history of this document according to AUTOSAR Release R25-11

A.1.1 Added Requirements in R25-11

none

A.1.2 Changed Requirements in R25-11

none

A.1.3 Deleted Requirements in R25-11

none

A.2 Traceable item history of this document according to AUTOSAR Release R24-11

A.2.1 Added Requirements in R24-11

none

A.2.2 Changed Requirements in R24-11

none

A.2.3 Deleted Requirements in R24-11

none

A.3 Traceable item history of this document according to AUTOSAR Release R23-11

A.3.1 Added Requirements in R23-11

none

A.3.2 Changed Requirements in R23-11

none

A.3.3 Deleted Requirements in R23-11

none