Document Title	Technical Report on Security Events Specification
Document Category	Technical report (TR)
Document UID	1122
Document Status	published
Part of AUTOSAR Standard	Foundation
Part of Standard Release	R26-11

Document Change History			
Date	**Release**	**Changed by**	**Description**
2026-11-26	R26-11	AUTOSAR Release Management	• Re-design of SOME/IP SEvs • Harmonization of SEvs between CP and AP • Rework of Chapter 4 table
2025-11-27	R25-11	AUTOSAR Release Management	• Added new Security Events for – DoIP – Identity & Access Management – Secure Boot • Changed Security Events for – Ethernet & TCP/IP – Firewall – SecOC – X.509 Certificates
2024-11-27	R24-11	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 Introduction 4
1.1 Objectives . . . 4
1.2 Document structure . . . 4
2 Definition of terms and acronyms 5
2.1 Acronyms and abbreviations . . . 5
3 Related Documentation 6
4 Security Event specification 7
5 Context data specification 13
5.1 Communication SEvs . . . 13
5.1.1 CAN SEvs . . . 13
5.1.2 Ethernet SEvs . . . 14
5.1.3 Firewall SEvs . . . 15
5.1.4 MACsec SEvs . . . 20
5.1.5 SecOC SEvs . . . 22
5.1.6 Signal-based communication SEvs . . . 22
5.1.7 TCPIP SEvs . . . 23
5.1.8 TLS SEvs . . . 24
5.1.9 Time Synchronization SEvs . . . 26
5.2 Cryptography SEvs . . . 28
5.2.1 Certificates SEvs . . . 28
5.3 Diagnostic SEvs . . . 30
5.3.1 DoIP SEvs . . . 30
5.3.2 UDS SEvs . . . 32
5.4 Identity and Access Management SEvs . . . 39
5.5 IdsM SEvs . . . 41
5.6 SOMEIP SEvs . . . 42
5.7 SW Update SEvs . . . 44
5.8 Secure Boot SEvs . . . 44

1 Introduction

This technical report provides the Security Event (SEv) specification of the AUTOSAR Standard.

1.1 Objectives

Efficient intrusion detection is heavily relying on IDS sensors monitoring sensible resources and providing high-quality information to the Vehicle Security Operation Center (VSOC). AUTOSAR implements a set of IDS sensors as part of the AUTOSAR software specification, where the respective SEv specification can be found in the corresponding SWS documents. This document collects these AUTOSAR-specified SEvs and provides an overview on all SEvs that are defined in AUTOSAR, including their specification.

The SEv specification in this document is provided in the form of generated tables. The source of the generated tables is the document FO_MOD_GeneralDefinitions [1], which can be used as a machine-readable version of the SEv specification in the VSOC.

Please note that this document does not contain the trigger condition under which the SEv is raised by the AUTOSAR stack. The trigger condition can be found in the SWS document of the module that raises the respective SEv.

1.2 Document structure

This document is structured as follows:

- Chapter 4 contains a list of all SEvs defined by AUTOSAR in a tabular form. The list contains SEv ID, Name, Description and AUTOSAR module that raises the SEv, but no context data.
- Chapter 5 contains detailed SEv specification including the SEvs context data. The chapter contains only SEvs for which context data is specified.

2 Definition of terms and acronyms

2.1 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:
IDS	Intrusion Detection System
SEv	Security Event
VSOC	Vehicle Security Operation Center

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

3 Related Documentation

[1] Standardized M1 Models used for the Definition of AUTOSAR
AUTOSAR_FO_MOD_GeneralDefinitions

[2] Glossary
AUTOSAR_FO_TR_Glossary

[3] General Specification of Basic Software Modules
AUTOSAR_CP_SWS_BSWGeneral

[4] General Specification of Adaptive Platform
AUTOSAR_AP_SWS_General

[5] Specification of Intrusion Detection System Protocol
AUTOSAR_FO_PRS_IntrusionDetectionSystem

4 Security Event specification

This section provides an overview over all Security Events provided by AUTOSAR. The module shortnames can be found in [SWS_BSW_91001] [3] and [AP_SWS_GENERAL_90025] [4].

SEv Id	*Name*	*Description*	*Raised by the following modules*	*Context Data Version*
Communication SEvs				
6	SEV_DROP_PDU_RX_UDP	SoAd dropped a PDU. The PDU violates stack configuration and was received via a UDP socket.	CP: SoAd AP: n/a	n/a
7	SEV_DROP_MSG_RX_UDP_LENGTH	SoAd dropped a message. The message contains at least one PDU which violates stack configuration and was received via a UDP socket. The violation relates to the length of the PDUs compared to the overall length of the message.	CP: SoAd AP: n/a	n/a
8	SEV_DROP_MSG_RX_UDP_SOCKET	SoAd received a UDP message which violates stack configuration and was dropped. No suitable socket connection matching to configuration was found.	CP: SoAd AP: n/a	n/a
9	SEV_REJECTED_TCP_CONNECTION	SoAd rejected a TCP connection. The connection request violates stack configuration.	CP: SoAd AP: n/a	n/a
10	SEV_ARP_IP_ADDR_CONFLICT	Received local IP address in ARP reply for different MAC.	CP: TcpIp AP: core	1
11	SEV_TCP_DROP_INV_DEST_PORT	Dropped TCP packet because of invalid destination TCP-Port.	CP: TcpIp AP: core	1
12	SEV_UDP_DROP_INV_DEST_PORT	Dropped UDP packet because of invalid destination UDP-Port.	CP: TcpIp AP: core	1
13	SEV_IPV4_DROP_INV_DEST_ADDR	Dropped datagram because of invalid destination IPV4 address.	CP: TcpIp AP: core	1
14	SEV_IPV6_DROP_INV_DEST_ADDR	Dropped datagram because of invalid destination IPV6 address.	CP: TcpIp AP: core	1
15	SEV_ETH_DROP_UNKNOWN_ETHERTYPE	An ethernet datagram was dropped due the Ethertype is not known.	CP: EthIf AP: core	1
16	SEV_ETH_DROP_VLAN_DOUBLE_TAG	An ethernet datagram was dropped due to double VLAN tag.	CP: EthIf AP: core	1
17	SEV_ETH_DROP_INV_VLAN	An ethernet datagram was dropped due to an invalid CrtlIdx/VLAN.	CP: EthIf AP: core	1
18	SEV_ETH_DROP_MAC_COLLISION	Ethernet datagram was dropped because local MAC was same as source MAC in an incoming frame.	CP: EthIf AP: core	1
19	SEV_CAN_TX_ERROR_DETECTED	A transmission related error was detected. Depending on the context data this could indicate suspicious CAN activity.	CP: CanIf AP: n/a	1
20	SEV_CAN_RX_ERROR_DETECTED	A reception related error was detected. Depending on the context data this could indicate suspicious CAN activity.	CP: CanIf AP: n/a	1

▽

△

SEv Id	Name	Description	Raised by the following modules	Context Data Version
21	SEV_CAN_ERRORSTATE_PASSIVE	The CAN controller transitioned to state passive.	CP: CanIf AP: n/a	1
22	SEV_CAN_ERRORSTATE_BUSOFF	The CAN controller transitioned to state busoff.	CP: CanIf AP: n/a	1
44	SEV_SECOC_MAC_VERIFICATION_FAILED	MAC verification of a received PDU failed.	CP: SecOC AP: com	1
45	SEV_SECOC_FRESHNESS_NOT_OK	Failed to get freshness value from Fv M upon reception of a SecOC secured PDU. Depending on the freshness value management, this can be an indicator of a replay attack.	CP: SecOC AP: com	1
50	SEV_DROP_PDU_RX_TCP	SoAd dropped a PDU. The PDU violates stack configuration and was received via a TCP socket.	CP: SoAd AP: n/a	n/a
51	SEV_FW_PACKET_BLOCKED_IPV4_MISMATCH	A network packet was blocked due to a rule mismatch on IPv4 layer.	CP: Fw AP: fw	2
52	SEV_FW_PACKET_BLOCKED_IPV6_MISMATCH	A network packet was blocked due to a rule mismatch on IPv6 layer.	CP: Fw AP: fw	2
53	SEV_FW_PACKET_BLOCKED_ICMP_MISMATCH	A network packet was blocked due to a rule mismatch within the ICMP protocol.	CP: Fw AP: fw	2
54	SEV_FW_PACKET_BLOCKED_TCP_MISMATCH	A network packet was blocked due to a rule mismatch on TCP layer.	CP: Fw AP: fw	2
55	SEV_FW_PACKET_BLOCKED_UDP_MISMATCH	A network packet was blocked due to a rule mismatch on UDP layer.	CP: Fw AP: fw	2
56	SEV_FW_PACKET_BLOCKED_SOMEIP_MISMATCH	A network packet was blocked due to a rule mismatch in the SOME/IP protocol.	CP: Fw AP: fw	2
57	SEV_FW_PACKET_BLOCKED_SOMEIPSD_MISMATCH	A network packet was blocked due to a rule mismatch in the SOME/IP SD protocol.	CP: Fw AP: fw	2
58	SEV_FW_PACKET_BLOCKED_DDS_MISMATCH	A network packet was blocked due to a rule mismatch in the DDS-RTPS protocol.	CP: Fw AP: fw	2
59	SEV_FW_PACKET_BLOCKED_DOIP_MISMATCH	A network packet was blocked due to a rule mismatch in the DoIP protocol.	CP: Fw AP: fw	2
60	SEV_FW_PACKET_BLOCKED_GENERIC_MISMATCH	A network packet was blocked due to a rule mismatch on generic inspection level.	CP: Fw AP: fw	2
61	SEV_FW_PACKET_BLOCKED_TCP_MAXCONNECTIONS	A network packet was blocked due to the maximal number of open TCP connections was reached.	CP: Fw AP: fw	2
62	SEV_FW_PACKET_BLOCKED_TCP_TIMEOUT	A network packet was blocked due to TCP timeout.	CP: Fw AP: fw	2
63	SEV_FW_PACKET_BLOCKED_TCP_STATETRANSITION	A network packet was blocked due to an invalid TCP state transition.	CP: Fw AP: fw	2
64	SEV_FW_PACKET_BLOCKED_RATELIMIT	A network packet was blocked due to the rate limit was reached.	CP: Fw AP: fw	2
66	SEV_TSYN_CAN_ICV_GENERATION_FAILED	ICV generation for a FUP message has failed.	CP: CanTSyn AP: n/a	1
67	SEV_TSYN_CAN_ICV_VERIFICATION_FAILED	ICV verification of a FUP message has failed.	CP: CanTSyn AP: n/a	1
68	SEV_TSYN_CAN_FRESHNESS_NOT_AVAILABLE	Failed to get freshness value from Fv M.	CP: CanTSyn AP: n/a	1

▽

△

SEv Id	Name	Description	Raised by the following modules	Context Data Version
69	SEV_TSYN_CAN_MSG_SEQUENCE_ERROR	Failed to receive correct sequence of SYNC and FUP from the TimeMaster within (CanTSynGlobalTimeFollowUp Timeout).	CP: CanTSyn AP: n/a	1
70	SEV_TSYN_FR_ICV_GENERATION_FAILED	ICV generation for a Sync message has failed.	CP: FrTSyn AP: n/a	1
71	SEV_TSYN_FR_ICV_VERIFICATION_FAILED	ICV verification of a received Sync message has failed.	CP: FrTSyn AP: n/a	1
72	SEV_TSYN_FR_FRESHNESS_NOT_AVAILABLE	Failed to get freshness value from Fv M.	CP: FrTSyn AP: n/a	1
73	SEV_TSYN_ETH_ICV_GENERATION_FAILED	ICV generation for a Follow_Up message failed.	CP: EthTSyn AP: tsync	1
74	SEV_TSYN_ETH_ICV_VERIFICATION_FAILED	ICV verification of a received Follow_Up message failed.	CP: EthTSyn AP: tsync	1
75	SEV_TSYN_ETH_FRESHNESS_NOT_AVAILABLE	Failed to get freshness value from Fv M.	CP: EthTSyn AP: tsync	1
76	SEV_TSYN_ETH_MSG_SEQUENCE_ERROR	Failed to receive correct sequence of SYNC and FUP from the TimeMaster within (EthTSynGlobalTimeFollowUp Timeout).	CP: EthTSyn AP: tsync	1
77	SEV_FW_PACKET_BLOCKED_DATALINKLAYER_MISMATCH	A network packet was blocked due to a rule mismatch on data link layer.	CP: Fw AP: fw	2
78	SEV_MKA_AUTHENTICATION_FAILURE	Event triggered when the authentication during the MKA communication has failed (wrong CKN/CAK).	CP: Mka AP: core	1
79	SEV_MKA_TIMEOUT	Event triggered when the timeout for the MKA communication has expired.	CP: Mka AP: core	1
80	SEV_MKA_PORT_NOT_ENABLED	Event triggered when the indicated port for the MKA communication is not enable.	CP: Mka AP: core	1
81	SEV_MKA_CIPHER_SUITE_NOT_SUPPORTED	Event triggered when there is no Cipher Suite supported.	CP: Mka AP: core	1
82	SEV_MKA_PORT_NUMBER_CHANGE	Event triggered when during the MKA communication the port number has changed.	CP: Mka AP: core	1
83	SEV_FW_PACKET_BLOCKED_BY_PERSTREAMFILTERING	A network packet was blocked due to per-stream filtering in the switch.	CP: Fw AP: n/a	1
89	SEV_COM_RX_SIGNAL_VALUE_UNEXPECTED	Signal or group signal is received with unexpected value.	CP: Com AP: n/a	1
90	SEV_TLS_ERROR	An alert message (warning or fatal) was detected (either received or generated) by TLS.	CP: TcpIp AP: com	2
91	SEV_TLS_CONNECTION_ESTABLISHED	A TLS connection was successfully established.	CP: TcpIp AP: com	2
92	SEV_TLS_CONNECTION_CLOSED	A TLS connection was closed normally.	CP: TcpIp AP: com	2
Cryptography SEvs				
5	SEV_CERT_CHAIN_VERIFICATION_FAILED	The verification of a certificate against a certificate chain was not successful.	CP: KeyM AP: crypto	2
95	SEV_CERT_INSTALL	Attempt to install a new certificate.	CP: KeyM AP: crypto	1

▽

△

SEv Id	Name	Description	Raised by the following modules	Context Data Version
96	SEV_CERT_UPDATE	Attempt to update a certificate.	CP: KeyM AP: crypto	1
97	SEV_CERT_DELETE	Attempt to delete a certificate.	CP: KeyM AP: crypto	1
98	SEV_CERT_INSTALLED_BUT_INVALID	An already installed certificate is invalid.	CP: KeyM AP: n/a	1
Diagnostic SEvs				
100	SEV_UDS_SECURITY_ACCESS_NEEDED	Tester has sent a diagnostic request without meeting the server's security level requirements for that service. NRC 0x33 (securityAccessDenied) was returned.	CP: Dcm AP: diag	1
101	SEV_UDS_AUTHENTICATION_NEEDED	A diagnostic request was received while the required authentication to execute this service is not given. NRC 0x34 (authenticationRequired) was returned.	CP: Dcm AP: diag	1
102	SEV_UDS_SECURITY_ACCESS_SUCCESSFUL	Successful unlocked the ECU (via Security Access SID 0x27)	CP: Dcm AP: diag	1
103	SEV_UDS_SECURITY_ACCESS_FAILED	Unlocking of the ECU (via Security Access SID 0x27) failed	CP: Dcm AP: diag	1
104	SEV_UDS_AUTHENTICATION_SUCCESSFUL	Succesfully authenticated (via Authentication SID 0x29)	CP: Dcm AP: diag	1
105	SEV_UDS_AUTHENTICATION_FAILED	Authentication (via Authentication SID 0x29) failed	CP: Dcm AP: diag	1
106	SEV_UDS_WRITE_DATA_SUCCESSFUL	Diagnostic data identifier has been written by SID 0x2E WriteDataBy Identifier	CP: Dcm AP: diag	1
107	SEV_UDS_WRITE_DATA_FAILED	Change of Diagnostic data identifier has been requested by SID 0x2E WriteDataByIdentifier, but failed	CP: Dcm AP: diag	1
108	SEV_UDS_WRITE_MEMORY_SUCCESSFUL	Data has been written into memory by SID 0x3D WriteMemoryByAddress	CP: Dcm AP: n/a	2
109	SEV_UDS_WRITE_MEMORY_FAILED	Writting of Data into memory has been requested by SID 0x3D WriteMemory ByAddress, but failed	CP: Dcm AP: n/a	2
110	SEV_UDS_REQUEST_UP_DOWNLOAD_SUCCESSFUL	An upload / download sequence has been requested successfully with SID 0x34 or SID 0x35	CP: Dcm AP: diag	2
111	SEV_UDS_REQUEST_UP_DOWNLOAD_FAILED	An upload / download sequence has been requested with SID 0x34 or SID 0x35, but failed	CP: Dcm AP: diag	2
112	SEV_UDS_REQUEST_FILE_TRANSFER_SUCCESSFUL	A file transfer sequence has been requested successfully with SID 0x38.	CP: Dcm AP: diag	1
113	SEV_UDS_REQUEST_FILE_TRANSFER_FAILED	A file transfer sequence has been requested with SID 0x38, but failed	CP: Dcm AP: diag	1
114	SEV_UDS_COMMUNICATION_CONTROL_SUCCESSFUL	The control of a communication has been requested by service SID 0x28 CommunicationControl successfully.	CP: Dcm AP: diag	1
115	SEV_UDS_COMMUNICATION_CONTROL_FAILED	The control of a communication has been requested by service SID 0x28 CommunicationControl, but failed.	CP: Dcm AP: diag	1

▽

△

SEv Id	Name	Description	Raised by the following modules	Context Data Version
116	SEV_UDS_CLEAR_DTC_SUCCESSFUL	DTC information has been cleared by SID 0x14 ClearDiagnosticInformation.	CP: Dcm AP: diag	1
117	SEV_UDS_CLEAR_DTC_FAILED	Clearing DTC information has been requested by SID 0x14 Clear DiagnosticInformation, but failed.	CP: Dcm AP: diag	1
118	SEV_UDS_CONTROL_DTC_SETTING_SUCCESSFUL	The control of a DTC setting has been requested by service SID 0x85 ControlDTCSetting successfully.	CP: Dcm AP: diag	1
119	SEV_UDS_CONTROL_DTC_SETTING_FAILED	Control of DTC setting has been requested by service SID 0x85 ControlDTCSetting, but failed.	CP: Dcm AP: diag	1
120	SEV_UDS_ECU_RESET_SUCCESSFUL	ECU has been reset by SID 0x11 ECUReset.	CP: Dcm AP: diag	1
121	SEV_UDS_ECU_RESET_FAILED	ECU Reset has been requested by SID 0x11 ECUReset, but failed.	CP: Dcm AP: diag	1
122	SEV_UDS_ROUTINE_CONTROL_SUCCESSFUL	The control of a routine has been requested by service SID 0x31 RoutineControl successfully.	CP: Dcm AP: diag	1
123	SEV_UDS_ROUTINE_CONTROL_FAILED	The control of a routine has been requested by service SID 0x31 RoutineControl, but failed.	CP: Dcm AP: diag	1
124	SEV_UDS_IO_CONTROL_SUCCESSFUL	IOControl operation has been requested by service SID 0x2F Input OutputControlByIdentifier successfully.	CP: Dcm AP: n/a	1
125	SEV_UDS_IO_CONTROL_FAILED	IOControl operation has been requested by service SID 0x2F Input OutputControlByIdentifier, but failed.	CP: Dcm AP: n/a	1
127	SEV_DOIP_HEADER_CHECK_FAILED	The DoIP Header Handler rejected a request (routing or diagnostic message).	CP: DoIP AP: diag	1
128	SEV_DOIP_ROUTING_ACTIVATION_CHECK_FAILED	A routing request was rejected by the routing handler.	CP: DoIP AP: diag	1
129	SEV_DOIP_ROUTING_ACTIVATION_SUCCESS	A routing request was successful.	CP: DoIP AP: diag	1
130	SEV_DOIP_DIAG_MESSAGE_CHECK_FAILED	A diagnostic message request was rejected by the diagnostic message handler.	CP: DoIP AP: diag	1
Identity and Access Management SEvs				
65	SEV_ACCESS_CONTROL_PHM_IAM_ACCESS_DENIED	Access of an application to a resource provided by Platform Health Management was denied.	CP: n/a AP: phm	1
131	SEV_ACCESS_CONTROL_FIREWALL_IAM_ACCESS_DENIED	Access of an application to a resource provided by the firewall was denied.	CP: n/a AP: fw	1
133	SEV_ACCESS_CONTROL_DM_IAM_ACCESS_DENIED	Access of an application to a resource provided by DM was denied.	CP: n/a AP: diag	1
134	SEV_ACCESS_CONTROL_CRYPTO_IAM_ACCESS_DENIED	Access of an application to a resource provided by Cryptography was denied.	CP: n/a AP: crypto	1
135	SEV_ACCESS_CONTROL_COM_IAM_ACCESS_DENIED	Access of an application to a resource provided by Communication Management was denied.	CP: n/a AP: com	1

▽

△

SEv Id	Name	Description	Raised by the following modules	Context Data Version
136	SEV_ACCESS_CONTROL_IDSM_IAM_ACCESS_DENIED	Access of an application to a resource provided by Intrusion Detection System Management was denied.	CP: n/a AP: idsm	1
137	SEV_ACCESS_CONTROL_SM_IAM_ACCESS_DENIED	Access of an application to a resource provided by State Management was denied.	CP: n/a AP: sm	1
IdsM SEvs				
46	SEV_IDSM_NO_EVENT_BUFFER_AVAILABLE	A SEv cannot be handled because there are no more event buffers available to process the event.	CP: IdsM AP: idsm	n/a
47	SEV_IDSM_NO_CONTEXT_DATA_BUFFER_AVAILABLE	The context data of an incoming event cannot be stored because there are no more context data buffers available.	CP: IdsM AP: idsm	n/a
49	SEV_IDSM_COMMUNICATION_ERROR	An error occurred when sending a QSEv via PDU.	CP: IdsM AP: idsm	n/a
87	SEV_IDSM_NO_QUALIFIED_EVENT_BUFFER_AVAILABLE	A security event raised when a QSEv has to be dropped due to insufficient QSEv buffers available.	CP: IdsM AP: idsm	n/a
126	SEV_IDSM_STATISTICS	A SEV reported by application to snapshot the IdsM statistics data.	CP: IdsM AP: n/a	1
SOMEIP SEvs				
138	SEV_SOMEIP_ERROR	The processing of a SOME/IP message resulted in a return not equal to E_OK.	CP: SomeIpXf AP: com	1
139	SEV_SOMEIP_UNAUTH_SERVICE_OFFER	A service offer was received from a server that is not authorized to offer it, or a service offer was received for a service that has already been offered by a different server.	CP: Sd AP: com	1
140	SEV_SOMEIP_SERVICE_NOT_AVAILABLE	A client invoked a method or attempted to subscribe to a eventgroup that does not belong to a currently offered service.	CP: Sd AP: com	1
141	SEV_SOMEIPSD_PDU_MALFORMED	The SOME/IP-SD length information of a received PDU violates the protocol definition.	CP: Sd AP: com	1
142	SEV_SOMEIP_UNAUTH_SUBSCRIPTION_REQ	A client attempted to subscribe to an eventgroup for which it is not authorized.	CP: Sd AP: com	1
143	SEV_SOMEIP_UNAUTH_METHOD_INVOCATION	A client attempted to invoke a method for which it is not authorized.	CP: Sd AP: com	1
SW Update SEvs				
93	SEV_SW_UPDATE_FAILED	A SW update operation was requested, but it was not successful.	CP: n/a AP: ucm	1
94	SEV_SW_UPDATE_SUCCESS	A SW update operation was executed successfully.	CP: n/a AP: ucm	1
Secure Boot SEvs				
99	SEV_EXEC_SW_COMPONENT_INTEGRITY_CHECK_FAILED	The integrity check of a SW component has failed.	CP: Crypto AP: core	1

Table 4.1: Security Events

5 Context data specification

This chapter lists the context data definition for all Security Events where context data is defined. Note that following [PRS_Ids_00004] all context data elements are provided in big endian byte order [5].

5.1 Communication SEvs

5.1.1 CAN SEvs

[SWS_CANIF_92000]

SEV Name	***SEV_CAN_TX_ERROR_DETECTED***	
ID	19	
Description	A transmission related error was detected. Depending on the context data this could indicate suspicious CAN activity.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
ControllerId	uint8	
CanError	uint8	CAN_ERROR_BIT_MONITORING1 (0x01) CAN_ERROR_BIT_MONITORING0 (0x02) CAN_ERROR_BIT (0x03) CAN_ERROR_CHECK_ACK_FAILED (0x04) CAN_ERROR_ACK_DELIMITER (0x05) CAN_ERROR_ARBITRATION_LOST (0x06) CAN_ERROR_OVERLOAD (0x07)

[SWS_CANIF_92001]

SEV Name	***SEV_CAN_RX_ERROR_DETECTED***	
ID	20	
Description	A reception related error was detected. Depending on the context data this could indicate suspicious CAN activity.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
ControllerId	uint8	
CanError	uint8	CAN_ERROR_CHECK_FORM_FAILED (0x08) CAN_ERROR_CHECK_STUFFING_FAILED (0x09) CAN_ERROR_CHECK_CRC_FAILED (0x0A) CAN_ERROR_BUS_LOOK (0x0B)

[SWS_CANIF_92002]

SEV Name	***SEV_CAN_ERRORSTATE_PASSIVE***	
ID	21	
Description	The CAN controller transitioned to state passive.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***

▽

△

SEV Name	*SEV_CAN_ERRORSTATE_PASSIVE*	
ControllerId	uint8	
ErrorCounterThreshold	uint8	0x00: TxErrorCounter > 127 AND RxErrorCounter > 127 0x01: TxErrorCounter > 127 AND RxErrorCounter < 127 0x02: TxErrorCounter < 127 AND RxErrorCounter > 127

[SWS_CANIF_92003]

SEV Name	*SEV_CAN_ERRORSTATE_BUSOFF*	
ID	22	
Description	The CAN controller transitioned to state busoff.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
ControllerId	uint8	

5.1.2 Ethernet SEvs

[SWS_APBSW_00100]
[SWS_EthIf_00699]

SEV Name	*SEV_ETH_DROP_UNKNOWN_ETHERTYPE*	
ID	15	
Description	An ethernet datagram was dropped due the Ethertype is not known.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	EthernetFrame, truncated to the first EthIfSEvEthernet FrameMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[SWS_APBSW_00101]
[SWS_EthIf_00701]

SEV Name	*SEV_ETH_DROP_VLAN_DOUBLE_TAG*	
ID	16	
Description	An ethernet datagram was dropped due to double VLAN tag.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	EthernetFrame, truncated to the first EthIfSEvEthernet FrameMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[SWS_APBSW_00102]
[SWS_EthIf_00703]

SEV Name	*SEV_ETH_DROP_INV_VLAN*	
ID	17	
Description	An ethernet datagram was dropped due to an invalid CrtlIdx/VLAN.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	EthernetFrame, truncated to the first EthIfSEvEthernet FrameMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[SWS_APBSW_00103]
[SWS_EthIf_00705]

SEV Name	*SEV_ETH_DROP_MAC_COLLISION*	
ID	18	
Description	Ethernet datagram was dropped because local MAC was same as source MAC in an incoming frame.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	EthernetFrame, truncated to the first EthIfSEvEthernet FrameMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

5.1.3 Firewall SEvs

[AP_SWS_Fw_60020]
[CP_SWS_Fw_60020]

SEV Name	*SEV_FW_PACKET_BLOCKED_IPV4_MISMATCH*	
ID	51	
Description	A network packet was blocked due to a rule mismatch on IPv4 layer.	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60021]
[CP_SWS_Fw_60021]

SEV Name	***SEV_FW_PACKET_BLOCKED_IPV6_MISMATCH***	
ID	52	
Description	A network packet was blocked due to a rule mismatch on IPv6 layer.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60022]
[CP_SWS_Fw_60022]

SEV Name	***SEV_FW_PACKET_BLOCKED_ICMP_MISMATCH***	
ID	53	
Description	A network packet was blocked due to a rule mismatch within the ICMP protocol.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60023]
[CP_SWS_Fw_60023]

SEV Name	***SEV_FW_PACKET_BLOCKED_TCP_MISMATCH***	
ID	54	
Description	A network packet was blocked due to a rule mismatch on TCP layer.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60024]
[CP_SWS_Fw_60024]

SEV Name	***SEV_FW_PACKET_BLOCKED_UDP_MISMATCH***	
ID	55	
Description	A network packet was blocked due to a rule mismatch on UDP layer.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60025]
[CP_SWS_Fw_60025]

SEV Name	***SEV_FW_PACKET_BLOCKED_SOMEIP_MISMATCH***	
ID	56	
Description	A network packet was blocked due to a rule mismatch in the SOME/IP protocol.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60026]
[CP_SWS_Fw_60026]

SEV Name	***SEV_FW_PACKET_BLOCKED_SOMEIPSD_MISMATCH***	
ID	57	
Description	A network packet was blocked due to a rule mismatch in the SOME/IP SD protocol.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60027]
[CP_SWS_Fw_60027]

SEV Name	***SEV_FW_PACKET_BLOCKED_DDS_MISMATCH***	
ID	58	
Description	A network packet was blocked due to a rule mismatch in the DDS-RTPS protocol.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60028]
[CP_SWS_Fw_60028]

SEV Name	***SEV_FW_PACKET_BLOCKED_DOIP_MISMATCH***	
ID	59	
Description	A network packet was blocked due to a rule mismatch in the DoIP protocol.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60029]
[CP_SWS_Fw_60029]

SEV Name	***SEV_FW_PACKET_BLOCKED_GENERIC_MISMATCH***	
ID	60	
Description	A network packet was blocked due to a rule mismatch on generic inspection level.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60002]
[CP_SWS_Fw_60002]

SEV Name	***SEV_FW_PACKET_BLOCKED_TCP_MAXCONNECTIONS***	
ID	61	
Description	A network packet was blocked due to the maximal number of open TCP connections was reached.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60030]
[CP_SWS_Fw_60030]

SEV Name	***SEV_FW_PACKET_BLOCKED_TCP_TIMEOUT***	
ID	62	
Description	A network packet was blocked due to TCP timeout.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60031]
[CP_SWS_Fw_60031]

SEV Name	***SEV_FW_PACKET_BLOCKED_TCP_STATETRANSITION***	
ID	63	
Description	A network packet was blocked due to an invalid TCP state transition.	
Context Data Version	2	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to - CP: FwSEvEthernetFrameMaxLength - AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract

▽

△

SEV Name	SEV_FW_PACKET_BLOCKED_TCP_STATETRANSITION	
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[AP_SWS_Fw_60003]
[CP_SWS_Fw_60003]

SEV Name	SEV_FW_PACKET_BLOCKED_RATELIMIT	
ID	64	
Description	A network packet was blocked due to the rate limit was reached.	
Context Data Version	2	
Context Data	Data Type	Allowed Values
MAC_Address	uint8 [6]	

[AP_SWS_Fw_60001]
[CP_SWS_Fw_60001]

SEV Name	SEV_FW_PACKET_BLOCKED_DATALINKLAYER_MISMATCH	
ID	77	
Description	A network packet was blocked due to a rule mismatch on data link layer.	
Context Data Version	2	
Context Data	Data Type	Allowed Values
Length	uint16	Length of EthernetFrame byte array
EthernetFrame	uint8 [54]	Received EthernetFrame, truncated to the first bytes according to • CP: FwSEvEthernetFrameMaxLength • AP: maxLength of the ContextDataElement Ethernet Frame from the SecurityExtract
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EthernetFrame byte array definition above.

[CP_SWS_Fw_60032]

SEV Name	SEV_FW_PACKET_BLOCKED_BY_PERSTREAMFILTERING	
ID	83	
Description	A network packet was blocked due to per-stream filtering in the switch.	
Context Data Version	1	
Context Data	Data Type	Allowed Values
BucketId	uint8	
CountValue	uint32	

5.1.4 MACsec SEvs

[CP_SWS_Mka_00309]
[SWS_APBSW_00500]

SEV Name	*SEV_MKA_AUTHENTICATION_FAILURE*	
ID	78	
Description	Event triggered when the authentication during the MKA communication has failed (wrong CKN/CAK).	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
PortId	uint8 [2]	
CKN	uint8 [32]	
MACAdressOfPeer	uint8 [6]	

[CP_SWS_Mka_00310]
[SWS_APBSW_00501]

SEV Name	*SEV_MKA_TIMEOUT*	
ID	79	
Description	Event triggered when the timeout for the MKA communication has expired.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
PortId	uint8 [2]	
CKN	uint8 [32]	
MACAdressOfPeer	uint8 [6]	

[CP_SWS_Mka_00311]
[SWS_APBSW_00502]

SEV Name	*SEV_MKA_PORT_NOT_ENABLED*	
ID	80	
Description	Event triggered when the indicated port for the MKA communication is not enable.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
PortId	uint8 [2]	
CKN	uint8 [32]	
MACAdressOfPeer	uint8 [6]	

[CP_SWS_Mka_00312]
[SWS_APBSW_00503]

SEV Name	*SEV_MKA_CIPHER_SUITE_NOT_SUPPORTED*	
ID	81	
Description	Event triggered when there is no Cipher Suite supported.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
PortId	uint8 [2]	
CKN	uint8 [32]	
MACAdressOfPeer	uint8 [6]	

[CP_SWS_Mka_00313]
[SWS_APBSW_00504]

SEV Name	*SEV_MKA_PORT_NUMBER_CHANGE*	
ID	82	
Description	Event triggered when during the MKA communication the port number has changed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
PortId	uint8 [2]	
CKN	uint8 [32]	
MACAdressOfPeer	uint8 [6]	

5.1.5 SecOC SEvs

[SWS_CM_11415]
[SWS_SecOC_92000]

SEV Name	*SEV_SECOC_MAC_VERIFICATION_FAILED*	
ID	44	
Description	MAC verification of a received PDU failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
DataId	uint16	

[SWS_CM_11416]
[SWS_SecOC_92001]

SEV Name	*SEV_SECOC_FRESHNESS_NOT_OK*	
ID	45	
Description	Failed to get freshness value from FvM upon reception of a SecOC secured PDU. Depending on the freshness value management, this can be an indicator of a replay attack.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
DataId	uint16	

5.1.6 Signal-based communication SEvs

[SWS_Com_00903]

SEV Name	*SEV_COM_RX_SIGNAL_VALUE_UNEXPECTED*	
ID	89	
Description	Signal or group signal is received with unexpected value.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
ComHandleId	uint16	

5.1.7 TCPIP SEvs

[SWS_APBSW_00300]
[SWS_Tcpip_00422]

SEV Name	***SEV_ARP_IP_ADDR_CONFLICT***	
ID	10	
Description	Received local IP address in ARP reply for different MAC.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of ReceivedPacket byte array
ReceivedPacket	uint8 [54]	Received Packet, truncated to the first TcpIpSEvReceived PacketMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the ReceivedPacket byte array definition above.

[SWS_APBSW_00301]
[SWS_Tcpip_00423]

SEV Name	***SEV_TCP_DROP_INV_DEST_PORT***	
ID	11	
Description	Dropped TCP packet because of invalid destination TCP-Port.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of ReceivedPacket byte array
ReceivedPacket	uint8 [54]	Received Packet, truncated to the first TcpIpSEvReceived PacketMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the ReceivedPacket byte array definition above.

[SWS_APBSW_00302]
[SWS_Tcpip_00424]

SEV Name	***SEV_UDP_DROP_INV_DEST_PORT***	
ID	12	
Description	Dropped UDP packet because of invalid destination UDP-Port.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
Length	uint16	Length of ReceivedPacket byte array
ReceivedPacket	uint8 [54]	Received Packet, truncated to the first TcpIpSEvReceived PacketMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the ReceivedPacket byte array definition above.

[SWS_APBSW_00303]
[SWS_Tcpip_00425]

SEV Name	*SEV_IPV4_DROP_INV_DEST_ADDR*	
ID	13	
Description	Dropped datagram because of invalid destination IPV4 address.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Length	uint16	Length of ReceivedPacket byte array
ReceivedPacket	uint8 [54]	Received Packet, truncated to the first TcpIpSEvReceived PacketMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the ReceivedPacket byte array definition above.

[SWS_APBSW_00304]
[SWS_TcpIp_00426]

SEV Name	*SEV_IPV6_DROP_INV_DEST_ADDR*	
ID	14	
Description	Dropped datagram because of invalid destination IPV6 address.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Length	uint16	Length of ReceivedPacket byte array
ReceivedPacket	uint8 [54]	Received Packet, truncated to the first TcpIpSEvReceived PacketMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the ReceivedPacket byte array definition above.

5.1.8 TLS SEvs

[SWS_CM_11417]
[SWS_TcpIp_00394]

SEV Name	*SEV_TLS_ERROR*	
ID	90	
Description	An alert message (warning or fatal) was detected (either received or generated) by TLS.	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
ReasonForFailure	uint8	Alert message as described in the the Alert Protocol in - RFC5246 for TLS Version 1.2 - RFC8446 for TLS Version 1.3 - RFC 6347 for DTLS Version 1.2 - RFC 9147 for DTLS Version 1.3
TLSVersion	uint16	Version as defined in RFC5246, RFC8446 - 0x0303 for TLS Version 1.2 - 0x0304 for TLS Version 1.3 - 0xFEFD for DTLS Version 1.2 - 0xFEFC for DTLS Version 1.3
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2

▽

△

SEV Name	*SEV_TLS_ERROR*	
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	

[SWS_CM_11418]
[SWS_TcpIp_00395]

SEV Name	*SEV_TLS_CONNECTION_ESTABLISHED*	
ID	91	
Description	A TLS connection was successfully established.	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
TLSVersion	uint16	Version as defined in RFC5246, RFC8446 - 0x0303 for TLS Version 1.2 - 0x0304 for TLS Version 1.3 - 0xFEFD for DTLS Version 1.2 - 0xFEFC for DTLS Version 1.3
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	

[SWS_CM_11419]
[SWS_TcpIp_00396]

SEV Name	*SEV_TLS_CONNECTION_CLOSED*	
ID	92	
Description	A TLS connection was closed normally.	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
ReasonForClosure	uint8	0: close_notify 90: user_canceled
TLSVersion	uint16	Version as defined in RFC5246, RFC8446 - 0x0303 for TLS Version 1.2 - 0x0304 for TLS Version 1.3 - 0xFEFD for DTLS Version 1.2 - 0xFEFC for DTLS Version 1.3
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	

5.1.9 Time Synchronization SEvs

[SWS_CanTSyn_92000]

SEV Name	*SEV_TSYN_CAN_ICV_GENERATION_FAILED*	
ID	66	
Description	ICV generation for a FUP message has failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_CanTSyn_92001]

SEV Name	*SEV_TSYN_CAN_ICV_VERIFICATION_FAILED*	
ID	67	
Description	ICV verification of a FUP message has failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_CanTSyn_92002]

SEV Name	*SEV_TSYN_CAN_FRESHNESS_NOT_AVAILABLE*	
ID	68	
Description	Failed to get freshness value from FvM.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_CanTSyn_92003]

SEV Name	*SEV_TSYN_CAN_MSG_SEQUENCE_ERROR*	
ID	69	
Description	Failed to receive correct sequence of SYNC and FUP from the TimeMaster within (CanTSyn GlobalTimeFollowUpTimeout).	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_FrTSyn_92000]

SEV Name	*SEV_TSYN_FR_ICV_GENERATION_FAILED*	
ID	70	
Description	ICV generation for a Sync message has failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_FrTSyn_92001]

SEV Name	*SEV_TSYN_FR_ICV_VERIFICATION_FAILED*	
ID	71	
Description	ICV verification of a received Sync message has failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_FrTSyn_92002]

SEV Name	*SEV_TSYN_FR_FRESHNESS_NOT_AVAILABLE*	
ID	72	
Description	Failed to get freshness value from FvM.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_EthTSyn_92000]
[SWS_TS_14214]

SEV Name	*SEV_TSYN_ETH_ICV_GENERATION_FAILED*	
ID	73	
Description	ICV generation for a Follow_Up message failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_EthTSyn_92001]
[SWS_TS_14215]

SEV Name	*SEV_TSYN_ETH_ICV_VERIFICATION_FAILED*	
ID	74	
Description	ICV verification of a received Follow_Up message failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_EthTSyn_92002]
[SWS_TS_14216]

SEV Name	*SEV_TSYN_ETH_FRESHNESS_NOT_AVAILABLE*	
ID	75	
Description	Failed to get freshness value from FvM.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

[SWS_EthTSyn_92003]
[SWS_TS_14217]

SEV Name	*SEV_TSYN_ETH_MSG_SEQUENCE_ERROR*	
ID	76	
Description	Failed to receive correct sequence of SYNC and FUP from the TimeMaster within (EthTSyn GlobalTimeFollowUpTimeout).	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GlobalTimeDomainId	uint8	

5.2 Cryptography SEvs

5.2.1 Certificates SEvs

[SWS_CRYPT_41059]
[SWS_KeyM_00307]

SEV Name	*SEV_CERT_CHAIN_VERIFICATION_FAILED*	
ID	5	
Description	The verification of a certificate against a certificate chain was not successful.	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
CertError	uint8	Cert_no_error (0x00) Cert_invalid_format (0x01) Cert_invalid_type (0x02) Cert_invalid_chain_of_trust (0x03) Cert_signature_fail (0x04) Cert_revoked (0x05) Cert_validity_period_fail (0x06) Cert_invalid_content (0x07) General_failure (0xFF)
Length	uint16	Length of Certificate byte array
Certificate	uint8 [100]	Certificate, optionally truncated to the first KeyMSEv CertificateMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the Certificate byte array definition above.

[SWS_CRYPT_41060]
[SWS_KeyM_00308]

SEV Name	*SEV_CERT_INSTALL*	
ID	95	
Description	Attempt to install a new certificate.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*

▽

△

SEV Name	*SEV_CERT_INSTALL*	
CertError	uint8	Cert_no_error (0x00) Cert_invalid_format (0x01) Cert_invalid_type (0x02) Cert_invalid_chain_of_trust (0x03) Cert_signature_fail (0x04) Cert_revoked (0x05) Cert_validity_period_fail (0x06) Cert_invalid_content (0x07) General_failure (0xFF)
Length	uint16	Length of Certificate byte array
Certificate	uint8 [100]	Certificate, optionally truncated to the first KeyMSEv CertificateMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the Certificate byte array definition above.

[SWS_CRYPT_41061]
[SWS_KeyM_00309]

SEV Name	*SEV_CERT_UPDATE*	
ID	96	
Description	Attempt to update a certificate.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
CertError	uint8	Cert_no_error (0x00) Cert_invalid_format (0x01) Cert_invalid_type (0x02) Cert_invalid_chain_of_trust (0x03) Cert_signature_fail (0x04) Cert_revoked (0x05) Cert_validity_period_fail (0x06) Cert_invalid_content (0x07) General_failure (0xFF)
Length	uint16	Length of Certificate byte array
Certificate	uint8 [100]	Certificate, optionally truncated to the first KeyMSEv CertificateMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the Certificate byte array definition above.

[SWS_CRYPT_41062]
[SWS_KeyM_00310]

SEV Name	*SEV_CERT_DELETE*	
ID	97	
Description	Attempt to delete a certificate.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*

▽

△

SEV Name	*SEV_CERT_DELETE*	
CertError	uint8	Cert_no_error (0x00) Cert_invalid_format (0x01) Cert_invalid_type (0x02) Cert_invalid_chain_of_trust (0x03) Cert_signature_fail (0x04) Cert_revoked (0x05) Cert_validity_period_fail (0x06) Cert_invalid_content (0x07) General_failure (0xFF)
Length	uint16	Length of Certificate byte array
Certificate	uint8 [100]	Certificate, optionally truncated to the first KeyMSEv CertificateMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the Certificate byte array definition above.

[SWS_KeyM_00311]

SEV Name	*SEV_CERT_INSTALLED_BUT_INVALID*	
ID	98	
Description	An already installed certificate is invalid.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
CertError	uint8	Cert_no_error (0x00) Cert_invalid_format (0x01) Cert_invalid_type (0x02) Cert_invalid_chain_of_trust (0x03) Cert_signature_fail (0x04) Cert_revoked (0x05) Cert_validity_period_fail (0x06) Cert_invalid_content (0x07) General_failure (0xFF)
Length	uint16	Length of Certificate byte array
Certificate	uint8 [100]	Certificate, optionally truncated to the first KeyMSEv CertificateMaxLength bytes
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the Certificate byte array definition above.

5.3 Diagnostic SEvs

5.3.1 DoIP SEvs

[SWS_DM_02135]
[SWS_DoIP_00511]

SEV Name	*SEV_DOIP_HEADER_CHECK_FAILED*	
ID	127	
Description	The DoIP Header Handler rejected a request (routing or diagnostic message).	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
SourceIp	uint8 [16]	
SourcePort	uint8 [2]	
ProtocolVersion	uint8 [1]	
PayloadType	uint8 [2]	
NACKCode	uint8 [1]	

[SWS_DM_02137] [SWS_DoIP_00512]

SEV Name	*SEV_DOIP_ROUTING_ACTIVATION_CHECK_FAILED*	
ID	128	
Description	A routing request was rejected by the routing handler.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
SourceIp	uint8 [16]	
SourcePort	uint8 [2]	
LogicalSourceAddress	uint8 [2]	
ActivationType	uint8 [1]	
ResponseCode	uint8 [1]	

[SWS_DM_02139] [SWS_DoIP_00513]

SEV Name	*SEV_DOIP_ROUTING_ACTIVATION_SUCCESS*	
ID	129	
Description	A routing request was successful.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
SourceIp	uint8 [16]	
SourcePort	uint8 [2]	
LogicalSourceAddress	uint8 [2]	
ActivationType	uint8 [1]	

[SWS_DM_02141] [SWS_DoIP_00514]

SEV Name	*SEV_DOIP_DIAG_MESSAGE_CHECK_FAILED*	
ID	130	
Description	A diagnostic message request was rejected by the diagnostic message handler.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*

▽

△

SEV Name	*SEV_DOIP_DIAG_MESSAGE_CHECK_FAILED*	
SourceIp	uint8 [16]	
SourcePort	uint8 [2]	
LogicalSourceAddress	uint8 [2]	
LogicalTargetAddress	uint8 [2]	
NACKCode	uint8 [1]	

5.3.2 UDS SEvs

[SWS_DM_02016]
[SWS_Dcm_01703]

SEV Name	*SEV_UDS_SECURITY_ACCESS_NEEDED*	
ID	100	
Description	Tester has sent a diagnostic request without meeting the server's security level requirements for that service. NRC 0x33 (securityAccessDenied) was returned.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
SID	uint8	
Subfunction	uint8	255: is filled in case the service is without Subfunction
DataIdentifier	uint16	65535: is filled in case the service is without DID
RoutineIdentifier	uint16	65535: is filled in case the service is without RID
ClientSourceAddress	uint16	

[SWS_DM_02018]
[SWS_Dcm_01705]

SEV Name	*SEV_UDS_AUTHENTICATION_NEEDED*	
ID	101	
Description	A diagnostic request was received while the required authentication to execute this service is not given. NRC 0x34 (authenticationRequired) was returned.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
SID	uint8	
Subfunction	uint8	255: is filled in case the service is without Subfunction
DataIdentifier	uint16	65535: is filled in case the service is without DID
RoutineIdentifier	uint16	65535: is filled in case the service is without RID
ClientSourceAddress	uint16	

[SWS_DM_02020]
[SWS_Dcm_01707]

SEV Name	*SEV_UDS_SECURITY_ACCESS_SUCCESSFUL*	
ID	102	
Description	Successful unlocked the ECU (via Security Access SID 0x27)	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Subfunction	uint8	
ClientSourceAddress	uint16	

[SWS_DM_02022]
[SWS_Dcm_01709]

SEV Name	*SEV_UDS_SECURITY_ACCESS_FAILED*	
ID	103	
Description	Unlocking of the ECU (via Security Access SID 0x27) failed	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Subfunction	uint8	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02024]
[SWS_Dcm_01711]

SEV Name	*SEV_UDS_AUTHENTICATION_SUCCESSFUL*	
ID	104	
Description	Succesfully authenticated (via Authentication SID 0x29)	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Subfunction	uint8	
ClientSourceAddress	uint16	

[SWS_DM_02026]
[SWS_Dcm_01713]

SEV Name	*SEV_UDS_AUTHENTICATION_FAILED*	
ID	105	
Description	Authentication (via Authentication SID 0x29) failed	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Subfunction	uint8	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02028]
[SWS_Dcm_01715]

SEV Name	*SEV_UDS_WRITE_DATA_SUCCESSFUL*	
ID	106	
Description	Diagnostic data identifier has been written by SID 0x2E WriteDataByIdentifier	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
DID	uint16	
ClientSourceAddress	uint16	

[SWS_DM_02030]
[SWS_Dcm_01717]

SEV Name	*SEV_UDS_WRITE_DATA_FAILED*	
ID	107	
Description	Change of Diagnostic data identifier has been requested by SID 0x2E WriteDataByIdentifier, but failed	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
DID	uint16	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_Dcm_01751]

SEV Name	*SEV_UDS_WRITE_MEMORY_SUCCESSFUL*	
ID	108	
Description	Data has been written into memory by SID 0x3D WriteMemoryByAddress	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
MemoryAddress	uint64	
MemorySize	uint64	
ClientSourceAddress	uint16	

[SWS_Dcm_01753]

SEV Name	*SEV_UDS_WRITE_MEMORY_FAILED*	
ID	109	
Description	Writting of Data into memory has been requested by SID 0x3D WriteMemoryByAddress, but failed	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
MemoryAddress	uint64	
MemorySize	uint64	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02032]
[SWS_Dcm_01719]

SEV Name	*SEV_UDS_REQUEST_UP_DOWNLOAD_SUCCESSFUL*	
ID	110	
Description	An upload / download sequence has been requested successfully with SID 0x34 or SID 0x35	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
SID	uint8	
MemoryAddress	uint64	
MemorySize	uint64	
ClientSourceAddress	uint16	

[SWS_DM_02034]
[SWS_Dcm_01721]

SEV Name	*SEV_UDS_REQUEST_UP_DOWNLOAD_FAILED*	
ID	111	
Description	An upload / download sequence has been requested with SID 0x34 or SID 0x35, but failed	
Context Data Version	2	
Context Data	*Data Type*	*Allowed Values*
SID	uint8	
MemoryAddress	uint64	
MemorySize	uint64	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02036]
[SWS_Dcm_01723]

SEV Name	*SEV_UDS_REQUEST_FILE_TRANSFER_SUCCESSFUL*	
ID	112	
Description	A file transfer sequence has been requested successfully with SID 0x38.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
ModeOfOperation	uint8	AddFile (0x01) DeleteFile (0x02) ReplaceFile (0x03) ReadFile (0x04) ReadDir (0x05) ResumeFile (0x06)
FilePathAndName	uint8 [50]	Each byte of this parameter is encoded in ASCII format.
ClientSourceAddress	uint16	

[SWS_DM_02038]
[SWS_Dcm_01725]

SEV Name	*SEV_UDS_REQUEST_FILE_TRANSFER_FAILED*
ID	113
Description	A file transfer sequence has been requested with SID 0x38, but failed
Context Data Version	1

▽

△

SEV Name	*SEV_UDS_REQUEST_FILE_TRANSFER_FAILED*	
Context Data	***Data Type***	***Allowed Values***
ModeOfOperation	uint8	AddFile (0x01) DeleteFile (0x02) ReplaceFile (0x03) ReadFile (0x04) ReadDir (0x05) ResumeFile (0x06)
FilePathAndName	uint8 [50]	Each byte of this parameter is encoded in ASCII format.
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02040]
[SWS_Dcm_01727]

SEV Name	*SEV_UDS_COMMUNICATION_CONTROL_SUCCESSFUL*	
ID	114	
Description	The control of a communication has been requested by service SID 0x28 Communication Control successfully.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
Subfunction	uint8	
ClientSourceAddress	uint16	

[SWS_DM_02042]
[SWS_Dcm_01729]

SEV Name	*SEV_UDS_COMMUNICATION_CONTROL_FAILED*	
ID	115	
Description	The control of a communication has been requested by service SID 0x28 Communication Control, but failed.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
Subfunction	uint8	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02044]
[SWS_Dcm_01731]

SEV Name	*SEV_UDS_CLEAR_DTC_SUCCESSFUL*	
ID	116	
Description	DTC information has been cleared by SID 0x14 ClearDiagnosticInformation.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
GroupOfDTC	uint8 [3]	given in the format: HighByte, MiddleByte, LowByte

▽

△

SEV Name	*SEV_UDS_CLEAR_DTC_SUCCESSFUL*	
MemorySelection	uint16	0x0001: PrimaryMemory 0x01XX: XX is the address of the UserDefinedMemory
ClientSourceAddress	uint16	

[SWS_DM_02046]
[SWS_Dcm_01733]

SEV Name	*SEV_UDS_CLEAR_DTC_FAILED*	
ID	117	
Description	Clearing DTC information has been requested by SID 0x14 ClearDiagnosticInformation, but failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
GroupOfDTC	uint8 [3]	given in the format: HighByte, MiddleByte, LowByte
MemorySelection	uint16	0x0001: PrimaryMemory 0x01XX: XX is the address of the UserDefinedMemory
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02048]
[SWS_Dcm_01735]

SEV Name	*SEV_UDS_CONTROL_DTC_SETTING_SUCCESSFUL*	
ID	118	
Description	The control of a DTC setting has been requested by service SID 0x85 ControlDTCSetting successfully.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Subfunction	uint8	
ClientSourceAddress	uint16	

[SWS_DM_02050]
[SWS_Dcm_01737]

SEV Name	*SEV_UDS_CONTROL_DTC_SETTING_FAILED*	
ID	119	
Description	Control of DTC setting has been requested by service SID 0x85 ControlDTCSetting, but failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Subfunction	uint8	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02052]
[SWS_Dcm_01739]

SEV Name	*SEV_UDS_ECU_RESET_SUCCESSFUL*	
ID	120	
Description	ECU has been reset by SID 0x11 ECUReset.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Subfunction	uint8	
ClientSourceAddress	uint16	

[SWS_DM_02054]
[SWS_Dcm_01741]

SEV Name	*SEV_UDS_ECU_RESET_FAILED*	
ID	121	
Description	ECU Reset has been requested by SID 0x11 ECUReset, but failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Subfunction	uint8	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_DM_02056]
[SWS_Dcm_01743]

SEV Name	*SEV_UDS_ROUTINE_CONTROL_SUCCESSFUL*	
ID	122	
Description	The control of a routine has been requested by service SID 0x31 RoutineControl successfully.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
RID	uint16	
Subfunction	uint8	
ClientSourceAddress	uint16	

[SWS_DM_02058]
[SWS_Dcm_01745]

SEV Name	*SEV_UDS_ROUTINE_CONTROL_FAILED*	
ID	123	
Description	The control of a routine has been requested by service SID 0x31 RoutineControl, but failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
RID	uint16	
Subfunction	uint8	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

[SWS_Dcm_01747]

SEV Name	*SEV_UDS_IO_CONTROL_SUCCESSFUL*	
ID	124	
Description	IOControl operation has been requested by service SID 0x2F InputOutputControlBy Identifier successfully.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
DID	uint16	
inputOutputControlParameter	uint8	
ClientSourceAddress	uint16	

[SWS_Dcm_01749]

SEV Name	*SEV_UDS_IO_CONTROL_FAILED*	
ID	125	
Description	IOControl operation has been requested by service SID 0x2F InputOutputControlBy Identifier, but failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
DID	uint16	
inputOutputControlParameter	uint8	
ClientSourceAddress	uint16	
NegativeResponseCode	uint8	

5.4 Identity and Access Management SEvs

[AP_SWS_Fw_60032]

SEV Name	*SEV_ACCESS_CONTROL_FIREWALL_IAM_ACCESS_DENIED*	
ID	131	
Description	Access of an application to a resource provided by the firewall was denied.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
UserId	uint32	

[SWS_DM_02133]

SEV Name	*SEV_ACCESS_CONTROL_DM_IAM_ACCESS_DENIED*	
ID	133	
Description	Access of an application to a resource provided by DM was denied.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
UserId	uint32	

[SWS_CRYPT_41023]

SEV Name	*SEV_ACCESS_CONTROL_CRYPTO_IAM_ACCESS_DENIED*	
ID	134	
Description	Access of an application to a resource provided by Cryptography was denied.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
UserId	uint32	

[SWS_CM_00602]

SEV Name	*SEV_ACCESS_CONTROL_COM_IAM_ACCESS_DENIED*	
ID	135	
Description	Access of an application to a resource provided by Communication Management was denied.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
UserId	uint32	

[SWS_AIDSM_02001]

SEV Name	*SEV_ACCESS_CONTROL_IDSM_IAM_ACCESS_DENIED*	
ID	136	
Description	Access of an application to a resource provided by Intrusion Detection System Management was denied.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
UserId	uint32	

[SWS_SM_70001]

SEV Name	*SEV_ACCESS_CONTROL_SM_IAM_ACCESS_DENIED*	
ID	137	
Description	Access of an application to a resource provided by State Management was denied.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
UserId	uint32	

[SWS_PHM_01375]

SEV Name	*SEV_ACCESS_CONTROL_PHM_IAM_ACCESS_DENIED*	
ID	65	
Description	Access of an application to a resource provided by Platform Health Management was denied.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
UserId	uint32	

5.5 IdsM SEvs

[SWS_IdsM_03016]

SEV Name	*SEV_IDSM_STATISTICS*	
ID	126	
Description	A SEV reported by application to snapshot the IdsM statistics data.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
ControlField	uint8	The 8 Bit control field is used to describe the content of the context data in the following bytes.
InstanceStatisticsForEvents	uint8 [10]	(Optional) The instance statistics segment contains various types of counts for events in an IdsM instance, e.g., number of events received, transmitted and stored. This segment of the context data is optional and its availability is indicated by Bit0 of the ControlField.
InstanceStatisticsForEvent Buffers	uint8 [4]	(Optional) The instance statistics segment contains buffer fill level information that are collected for an IdsM instance, e.g., peak fill level of the event and qualified event buffers. This segment of the context data is optional and its availability is indicated by Bit0 of the ControlField.
InstanceStatisticsContext DataBuffer	uint8 [380]	(Optional) The instance statistics segment contains the peakfill level of all the unique context data buffers configured in IdsM. The field has a variable length because the IdsM provides the possibility to configure a wide-range of context data buffers of different sizes. The variable length in bytes is equal to 2 + (6 x Number of unique context data buffer sizes). This segment of the context data is optional and its availability is indicated by Bit0 of the ControlField. Note: Since IdsM supports maximum of 1500 bytes of context data (ECUC_IdsM_00047), the number unique context data buffers for which statistics collected is limited to 63. The maximum length for this field is 380 bytes (2 + (63 * 6) bytes).
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the InstanceStatisticsContextDataBuffer byte array definition above.
EventSpecificStatistics	uint8 [891]	(Optional) The event specific statistics segment contains individual counts of reception and qualifcation for select events. This segment of the context data is optional and has a variable length because IdsM provides the possibility to configure IdsMEventStatistics for every IdsMEvent. The variable length in bytes is equal to 2 + (7 x Number of IdsMEvent with IdsMEventStatistics set to TRUE). This segment of the context data is optional and its availability is indicated by Bit1 of the ControlField. Note: Since IdsM support maximum of 1500 bytes of context data (ECUC_IdsM_00047), the number of events for which statistics collected is limited to 127. The maximum length for this field is 891 (2 + (127 * 7) bytes).
	MAX-LENGTH	Truncation length can be defined on a project specific basis. AUTOSAR has defined a default value, as given in the EventSpecificStatistics byte array definition above.

5.6 SOMEIP SEvs

[SWS_CM_00243]
[SWS_SomeIpXf_00309]

SEV Name	*SEV_SOMEIP_ERROR*	
ID	138	
Description	The processing of a SOME/IP message resulted in a return not equal to E_OK.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	
SomeIpHeader	uint8 [16]	
ReturnCode	uint8	E_NOT_OK (0x01) E_UNKNOWN_SERVICE (0x02) E_UNKNOWN_METHOD (0x03) E_WRONG_PROTOCOL_VERSION (0x07) E_WRONG_INTERFACE_VERSION (0x08) E_MALFORMED_MESSAGE (0x09) E_WRONG_MESSAGE_TYPE (0x0A) E_E2E (0x0D)

[SWS_CM_00244]
[SWS_Sd_00808]

SEV Name	*SEV_SOMEIP_UNAUTH_SERVICE_OFFER*	
ID	139	
Description	A service offer was received from a server that is not authorized to offer it, or a service offer was received for a service that has already been offered by a different server.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	
SomeIpHeader	uint8 [16]	

[SWS_CM_00246]
[SWS_Sd_00809]

SEV Name	*SEV_SOMEIP_SERVICE_NOT_AVAILABLE*
ID	140
Description	A client invoked a method or attempted to subscribe to a eventgroup that does not belong to a currently offered service.
Context Data Version	1

▽

△

SEV Name	*SEV_SOMEIP_SERVICE_NOT_AVAILABLE*	
Context Data	***Data Type***	***Allowed Values***
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	
SomeIpHeader	uint8 [16]	

[SWS_CM_00247]
[SWS_Sd_00810]

SEV Name	*SEV_SOMEIPSD_PDU_MALFORMED*	
ID	141	
Description	The SOME/IP-SD length information of a received PDU violates the protocol definition.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	
SomeIpHeader	uint8 [16]	

[SWS_CM_00248]
[SWS_Sd_00811]

SEV Name	*SEV_SOMEIP_UNAUTH_SUBSCRIPTION_REQ*	
ID	142	
Description	A client attempted to subscribe to an eventgroup for which it is not authorized.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	
SomeIpHeader	uint8 [16]	

[SWS_CM_00261]
[SWS_Sd_00812]

SEV Name	*SEV_SOMEIP_UNAUTH_METHOD_INVOCATION*	
ID	143	
Description	A client attempted to invoke a method for which it is not authorized.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
SourceIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
SourcePort	uint16	
DestinationIpAddress	uint8 [16]	All IPv6 addresses and IPv4 addresses shall be encoded as specified in RFC 4291 Section 2.5.5.2
DestinationPort	uint16	
SomeIpHeader	uint8 [16]	

5.7 SW Update SEvs

[SWS_UCM_00404]

SEV Name	*SEV_SW_UPDATE_FAILED*	
ID	93	
Description	A SW update operation was requested, but it was not successful.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Action	uint8	
ErrorCode	uint8	
Resolution	uint8	
SwName	uint8 [128, encoding UTF-8]	
ReceivedSwVersion	uint8 [32, encoding UTF-8]	

[SWS_UCM_00405]

SEV Name	*SEV_SW_UPDATE_SUCCESS*	
ID	94	
Description	A SW update operation was executed successfully.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
Action	uint8	
SwName	uint8 [128, encoding UTF-8]	
ReceivedSwVersion	uint8 [32, encoding UTF-8]	

5.8 Secure Boot SEvs

[SWS_APBSW_00072]
[SWS_Crypto_00303]

SEV Name	***SEV_EXEC_SW_COMPONENT_INTEGRITY_CHECK_FAILED***	
ID	99	
Description	The integrity check of a SW component has failed.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***
SWComponent	uint16	
VerificationMode	uint8	RECOVERY (0x00) MEASURED_BOOT (0x01) RUNTIME_PERIODIC (0x02) STRICT (0x03)