Document Title	Technical Report on Security Events Specification
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	1122

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	• 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 15
5.1 Communication SEvs . . . 15
5.1.1 TLS . . . 15
5.1.2 MACsec . . . 16
5.1.3 SecOC . . . 17
5.1.4 Firewall . . . 18
5.1.5 CAN . . . 24
5.1.6 Ethernet . . . 25
5.1.7 TCP/IP . . . 26
5.1.8 Signal-based communication . . . 28
5.1.9 Time Synchronization . . . 28
5.2 Cryptography SEvs . . . 31
5.2.1 Certificates . . . 31
5.3 Diagnostic SEvs . . . 33
5.3.1 DoIP . . . 33
5.3.2 UDS . . . 35
5.4 Identity and Access Management SEvs . . . 43
5.5 Secure Boot SEvs . . . 44
5.6 SW Update SEvs . . . 45

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] Specification of Intrusion Detection System Protocol
AUTOSAR_FO_PRS_IntrusionDetectionSystem

4 Security Event specification

ID	Owner	Name	Description
5	KeyM	SEV_CERT_CHAIN_VERIFICATION_FAILED	The verification of a certificate against a certificate chain was not successful.
95	KeyM	SEV_CERT_INSTALL	Attempt to install a new certificate.
96	KeyM	SEV_CERT_UPDATE	Attempt to update a certificate.
97	KeyM	SEV_CERT_DELETE	Attempt to delete a certificate.
98	KeyM	SEV_CERT_INSTALLED_BUT_INVALID	An already installed certificate is invalid.
46	IdsM	SEV_IDSM_NO_EVENT_BUFFER_AVAILABLE	A SEv cannot be handled because there are no more event buffers available to process the event.
47	IdsM	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.
48	IdsM	SEV_IDSM_TRAFFIC_LIMITATION_EXCEEDED	The current traffic exceeds a configured traffic limitation.
49	IdsM	SEV_IDSM_COMMUNICATION_ERROR	An error occurred when sending a QSEv via PDU.
87	IdsM	SEV_IDSM_NO_QUALIFIED_EVENT_BUFFER_AVAILABLE	A security event raised when a QSEv has to be dropped due to insufficient QSEv buffers available.
46	AIDSM	SEV_IDSM_NO_EVENT_BUFFER_AVAILABLE	A SEv cannot be handled because there are no more event buffers available to process the event.
47	AIDSM	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.
48	AIDSM	SEV_IDSM_TRAFFIC_LIMITATION_EXCEEDED	The current traffic exceeds a configured traffic limitation.
49	AIDSM	SEV_IDSM_COMMUNICATION_ERROR	An error occurred when sending a QSEv via PDU.
87	AIDSM	SEV_IDSM_NO_QUALIFIED_EVENT_BUFFER_AVAILABLE	A security event raised when a QSEv has to be dropped due to insufficient QSEv buffers available.
136	AIDSM	SEV_ACCESS_CONTROL_IDSM_IAM_ACCESS_DENIED	Access of an application to a resource provided by Intrusion Detection System Management was denied.
89	Com	SEV_COM_RX_SIGNAL_VALUE_UNEXPECTED	Signal or group signal is received with unexpected value.
135	CM	SEV_ACCESS_CONTROL_COM_IAM_ACCESS_DENIED	Access of an application to a resource provided by Communication Management was denied.
15	EthIf	SEV_ETH_DROP_UNKNOWN_ETHERTYPE	An ethernet datagram was dropped due the Ethertype is not known.
16	EthIf	SEV_ETH_DROP_VLAN_DOUBLE_TAG	An ethernet datagram was dropped due to double VLAN tag.
17	EthIf	SEV_ETH_DROP_INV_VLAN	An ethernet datagram was dropped due to an invalid CrtlIdx/VLAN.
18	EthIf	SEV_ETH_DROP_MAC_COLLISION	Ethernet datagram was dropped because local MAC was same as source MAC in an incoming frame.
19	CANIF	SEV_CAN_TX_ERROR_DETECTED	A transmission related error was detected. Depending on the context data this could indicate suspicious CAN activity.

▽

△

ID	Owner	Name	Description
20	CANIF	SEV_CAN_RX_ERROR_DETECTED	A reception related error was detected. Depending on the context data this could indicate suspicious CAN activity.
21	CANIF	SEV_CAN_ERRORSTATE_PASSIVE	The CAN controller transitioned to state passive.
22	CANIF	SEV_CAN_ERRORSTATE_BUSOFF	The CAN controller transitioned to state busoff.
6	SoAd	SEV_DROP_PDU_RX_UDP	SoAd dropped a PDU. The PDU violates stack configuration and was received via a UDP socket.
7	SoAd	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.
8	SoAd	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.
9	SoAd	SEV_REJECTED_TCP_ CONNECTION	SoAd rejected a TCP connection. The connection request violates stack configuration.
50	SoAd	SEV_DROP_PDU_RX_TCP	SoAd dropped a PDU. The PDU violates stack configuration and was received via a TCP socket.
10	TcpIp	SEV_ARP_IP_ADDR_CONFLICT	Received local IP address in ARP reply for different MAC.
11	TcpIp	SEV_TCP_DROP_INV_DEST_PORT	Dropped TCP packet because of invalid destination TCP-Port.
12	TcpIp	SEV_UDP_DROP_INV_DEST_PORT	Dropped UDP packet because of invalid destination UDP-Port.
13	TcpIp	SEV_IPV4_DROP_INV_DEST_ ADDR	Dropped datagram because of invalid destination IPV4 address.
14	TcpIp	SEV_IPV6_DROP_INV_DEST_ ADDR	Dropped datagram because of invalid destination IPV6 address.
90	TcpIp	SEV_TLS_ERROR	An alert message (warning or fatal) was detected (either received or generated) by TLS.
91	TcpIp	SEV_TLS_CONNECTION_ ESTABLISHED	A TLS connection was successfully established.
92	TcpIp	SEV_TLS_CONNECTION_CLOSED	A TLS connection was closed normally.
44	SecOC	SEV_SECOC_MAC_VERIFICATION_ FAILED	MAC verification of a received PDU failed.
45	SecOC	SEV_SECOC_FRESHNESS_NOT_ OK	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.
51	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_ IPV4_MISMATCH	A network packet was blocked due to a rule mismatch on IPv4 layer.
52	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_ IPV6_MISMATCH	A network packet was blocked due to a rule mismatch on IPv6 layer.
53	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_ ICMP_MISMATCH	A network packet was blocked due to a rule mismatch within the ICMP protocol.
54	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_ TCP_MISMATCH	A network packet was blocked due to a rule mismatch on TCP layer.
55	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_ UDP_MISMATCH	A network packet was blocked due to a rule mismatch on UDP layer.

▽

△

ID	Owner	Name	Description
56	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_SOMEIP_MISMATCH	A network packet was blocked due to a rule mismatch in the SOME/IP protocol.
57	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_SOMEIPSD_MISMATCH	A network packet was blocked due to a rule mismatch in the SOME/IP SD protocol.
58	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_DDS_MISMATCH	A network packet was blocked due to a rule mismatch in the DDS-RTPS protocol.
59	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_DOIP_MISMATCH	A network packet was blocked due to a rule mismatch in the DoIP protocol.
60	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_GENERIC_MISMATCH	A network packet was blocked due to a rule mismatch on generic inspection level.
61	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_TCP_MAXCONNECTIONS	A network packet was blocked due to the maximal number of open TCP connections was reached.
62	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_TCP_TIMEOUT	A network packet was blocked due to TCP timeout.
63	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_TCP_STATETRANSITION	A network packet was blocked due to an invalid TCP state transition.
64	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_RATELIMIT	A network packet was blocked due to the rate limit was reached.
77	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_DATALINKLAYER_MISMATCH	A network packet was blocked due to a rule mismatch on data link layer.
83	CP_SWS_Fw	SEV_FW_PACKET_BLOCKED_BY_PERSTREAMFILTERING	A network packet was blocked due to per-stream filtering in the switch.
51	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_IPV4_MISMATCH	A network packet was blocked due to a rule mismatch on IPv4 layer.
52	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_IPV6_MISMATCH	A network packet was blocked due to a rule mismatch on IPv6 layer.
53	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_ICMP_MISMATCH	A network packet was blocked due to a rule mismatch within the ICMP protocol.
54	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_TCP_MISMATCH	A network packet was blocked due to a rule mismatch on TCP layer.
55	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_UDP_MISMATCH	A network packet was blocked due to a rule mismatch on UDP layer.
56	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_SOMEIP_MISMATCH	A network packet was blocked due to a rule mismatch in the SOME/IP protocol.
57	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_SOMEIPSD_MISMATCH	A network packet was blocked due to a rule mismatch in the SOME/IP SD protocol.
58	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_DDS_MISMATCH	A network packet was blocked due to a rule mismatch in the DDS-RTPS protocol.
59	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_DOIP_MISMATCH	A network packet was blocked due to a rule mismatch in the DoIP protocol.
60	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_GENERIC_MISMATCH	A network packet was blocked due to a rule mismatch on generic inspection level.
61	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_TCP_MAXCONNECTIONS	A network packet was blocked due to the maximal number of open TCP connections was reached.
62	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_TCP_TIMEOUT	A network packet was blocked due to TCP timeout.
63	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_TCP_STATETRANSITION	A network packet was blocked due to an invalid TCP state transition.
64	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_RATELIMIT	A network packet was blocked due to the rate limit was reached.

▽

△

ID	Owner	Name	Description
77	AP_SWS_Fw	SEV_FW_PACKET_BLOCKED_DATALINKLAYER_MISMATCH	A network packet was blocked due to a rule mismatch on data link layer.
131	AP_SWS_Fw	SEV_ACCESS_CONTROL_FIREWALL_IAM_ACCESS_DENIED	Access of an application to a resource provided by the firewall was denied.
66	CanTSyn	SEV_TSYN_CAN_ICV_GENERATION_FAILED	ICV generation for a FUP message has failed.
67	CanTSyn	SEV_TSYN_CAN_ICV_VERIFICATION_FAILED	ICV verification of a FUP message has failed.
68	CanTSyn	SEV_TSYN_CAN_FRESHNESS_NOT_AVAILABLE	Failed to get freshness value from FvM.
69	CanTSyn	SEV_TSYN_CAN_MSG_SEQUENCE_ERROR	Failed to receive correct sequence of SYNC and FUP from the TimeMaster within (CanTSyn GlobalTimeFollowUpTimeout).
70	FrTSyn	SEV_TSYN_FR_ICV_GENERATION_FAILED	ICV generation for a Sync message has failed.
71	FrTSyn	SEV_TSYN_FR_ICV_VERIFICATION_FAILED	ICV verification of a received Sync message has failed.
72	FrTSyn	SEV_TSYN_FR_FRESHNESS_NOT_AVAILABLE	Failed to get freshness value from FvM.
73	EthTSyn	SEV_TSYN_ETH_ICV_GENERATION_FAILED	ICV generation for a Follow_Up message failed.
74	EthTSyn	SEV_TSYN_ETH_ICV_VERIFICATION_FAILED	ICV verification of a received Follow_Up message failed.
75	EthTSyn	SEV_TSYN_ETH_FRESHNESS_NOT_AVAILABLE	Failed to get freshness value from FvM.
76	EthTSyn	SEV_TSYN_ETH_MSG_SEQUENCE_ERROR	Failed to receive correct sequence of SYNC and FUP from the TimeMaster within (EthTSyn GlobalTimeFollowUpTimeout).
73	TS	SEV_TSYN_ETH_ICV_GENERATION_FAILED	ICV generation for a Follow_Up message failed.
74	TS	SEV_TSYN_ETH_ICV_VERIFICATION_FAILED	ICV verification of a received Follow_Up message failed.
75	TS	SEV_TSYN_ETH_FRESHNESS_NOT_AVAILABLE	Failed to get freshness value from FvM.
76	TS	SEV_TSYN_ETH_MSG_SEQUENCE_ERROR	Failed to receive correct sequence of SYNC and FUP from the TimeMaster within (EthTSyn GlobalTimeFollowUpTimeout).
78	CP_SWS_Mka	SEV_MKA_AUTHENTICATION_FAILURE	Event triggered when the authentication during the MKA communication has failed (wrong CKN/CAK).
79	CP_SWS_Mka	SEV_MKA_TIMEOUT	Event triggered when the timeout for the MKA communication has expired.
80	CP_SWS_Mka	SEV_MKA_PORT_NOT_ENABLED	Event triggered when the indicated port for the MKA communication is not enable.
81	CP_SWS_Mka	SEV_MKA_CIPHER_SUITE_NOT_SUPPORTED	Event triggered when there is no Cipher Suite supported.
82	CP_SWS_Mka	SEV_MKA_PORT_NUMBER_CHANGE	Event triggered when during the MKA communication the port number has changed.
84	Sd	SEV_SOME_IP_ACL_CHECK_FAILED_OFFER	ACL check for a service offer failed.
85	Sd	SEV_SOME_IP_ACL_CHECK_FAILED_EVENT_SUBSCRIPTION	ACL check for a subscribe event group request failed.

▽

△

ID	Owner	Name	Description
86	Sd	SEV_SOME_IP_ACL_CHECK_FAILED_METHOD_REQUEST	ACL check for a method request failed.
88	Sd	SEV_SOME_IP_SD_DUPLICATE_OFFER	SD rejected Offer for a ServiceInstance which is already offered by a different endpoint and TTL still valid.
100	Dcm	SEV_UDS_SECURITY_ACCESS_NEEDED	Tester has sent a diagnostic request without meeting the server's security level requirements for that service. NRC 0x33 (securityAccess Denied) was returned.
101	Dcm	SEV_UDS_AUTHENTICATION_NEEDED	A diagnostic request was received while the required authentication to execute this service is not given. NRC 0x34 (authentication Required) was returned.
102	Dcm	SEV_UDS_SECURITY_ACCESS_SUCCESSFUL	Successful unlocked the ECU (via Security Access SID 0x27)
103	Dcm	SEV_UDS_SECURITY_ACCESS_FAILED	Unlocking of the ECU (via Security Access SID 0x27) failed
104	Dcm	SEV_UDS_AUTHENTICATION_SUCCESSFUL	Succesfully authenticated (via Authentication SID 0x29)
105	Dcm	SEV_UDS_AUTHENTICATION_FAILED	Authentication (via Authentication SID 0x29) failed
106	Dcm	SEV_UDS_WRITE_DATA_SUCCESSFUL	Diagnostic data identifier has been written by SID 0x2E WriteDataByIdentifier
107	Dcm	SEV_UDS_WRITE_DATA_FAILED	Change of Diagnostic data identifier has been requested by SID 0x2E WriteDataByIdentifier, but failed
108	Dcm	SEV_UDS_WRITE_MEMORY_SUCCESSFUL	Data has been written into memory by SID 0x3 D WriteMemoryByAddress
109	Dcm	SEV_UDS_WRITE_MEMORY_FAILED	Writting of Data into memory has been requested by SID 0x3D WriteMemoryBy Address, but failed
110	Dcm	SEV_UDS_REQUEST_UP_DOWNLOAD_SUCCESSFUL	An upload / download sequence has been requested successfully with SID 0x34 or SID 0x35
111	Dcm	SEV_UDS_REQUEST_UP_DOWNLOAD_FAILED	An upload / download sequence has been requested with SID 0x34 or SID 0x35, but failed
112	Dcm	SEV_UDS_REQUEST_FILE_TRANSFER_SUCCESSFUL	A file transfer sequence has been requested successfully with SID 0x38.
113	Dcm	SEV_UDS_REQUEST_FILE_TRANSFER_FAILED	A file transfer sequence has been requested with SID 0x38, but failed
114	Dcm	SEV_UDS_COMMUNICATION_CONTROL_SUCCESSFUL	The control of a communication has been requested by service SID 0x28 Communication Control successfully.
115	Dcm	SEV_UDS_COMMUNICATION_CONTROL_FAILED	The control of a communication has been requested by service SID 0x28 Communication Control, but failed.
116	Dcm	SEV_UDS_CLEAR_DTC_SUCCESSFUL	DTC information has been cleared by SID 0x14 ClearDiagnosticInformation.
117	Dcm	SEV_UDS_CLEAR_DTC_FAILED	Clearing DTC information has been requested by SID 0x14 ClearDiagnosticInformation, but failed.
118	Dcm	SEV_UDS_CONTROL_DTC_SETTING_SUCCESSFUL	The control of a DTC setting has been requested by service SID 0x85 Control DTCSetting successfully.

▽

△

ID	Owner	Name	Description
119	Dcm	SEV_UDS_CONTROL_DTC_SETTING_FAILED	Control of DTC setting has been requested by service SID 0x85 ControlDTCSetting, but failed.
120	Dcm	SEV_UDS_ECU_RESET_SUCCESSFUL	ECU has been reset by SID 0x11 ECUReset.
121	Dcm	SEV_UDS_ECU_RESET_FAILED	ECU Reset has been requested by SID 0x11 ECUReset, but failed.
122	Dcm	SEV_UDS_ROUTINE_CONTROL_SUCCESSFUL	The control of a routine has been requested by service SID 0x31 RoutineControl successfully.
123	Dcm	SEV_UDS_ROUTINE_CONTROL_FAILED	The control of a routine has been requested by service SID 0x31 RoutineControl, but failed.
124	Dcm	SEV_UDS_IO_CONTROL_SUCCESSFUL	IOControl operation has been requested by service SID 0x2F InputOutputControlByIdentifier successfully.
125	Dcm	SEV_UDS_IO_CONTROL_FAILED	IOControl operation has been requested by service SID 0x2F InputOutputControlByIdentifier, but failed.
100	DM	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.
101	DM	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.
102	DM	SEV_UDS_SECURITY_ACCESS_SUCCESSFUL	Successful unlocked the ECU (via Security Access SID 0x27)
103	DM	SEV_UDS_SECURITY_ACCESS_FAILED	Unlocking of the ECU (via Security Access SID 0x27) failed
104	DM	SEV_UDS_AUTHENTICATION_SUCCESSFUL	Succesfully authenticated (via Authentication SID 0x29)
105	DM	SEV_UDS_AUTHENTICATION_FAILED	Authentication (via Authentication SID 0x29) failed
106	DM	SEV_UDS_WRITE_DATA_SUCCESSFUL	Diagnostic data identifier has been written by SID 0x2E WriteDataByIdentifier
107	DM	SEV_UDS_WRITE_DATA_FAILED	Change of Diagnostic data identifier has been requested by SID 0x2E WriteDataByIdentifier, but failed
110	DM	SEV_UDS_REQUEST_UP_DOWNLOAD_SUCCESSFUL	An upload / download sequence has been requested successfully with SID 0x34 or SID 0x35
111	DM	SEV_UDS_REQUEST_UP_DOWNLOAD_FAILED	An upload / download sequence has been requested with SID 0x34 or SID 0x35, but failed
112	DM	SEV_UDS_REQUEST_FILE_TRANSFER_SUCCESSFUL	A file transfer sequence has been requested successfully with SID 0x38.
113	DM	SEV_UDS_REQUEST_FILE_TRANSFER_FAILED	A file transfer sequence has been requested with SID 0x38, but failed
114	DM	SEV_UDS_COMMUNICATION_CONTROL_SUCCESSFUL	The control of a communication has been requested by service SID 0x28 CommunicationControl successfully.
115	DM	SEV_UDS_COMMUNICATION_CONTROL_FAILED	The control of a communication has been requested by service SID 0x28 CommunicationControl, but failed.
116	DM	SEV_UDS_CLEAR_DTC_SUCCESSFUL	DTC information has been cleared by SID 0x14 ClearDiagnosticInformation.

▽

△

ID	*Owner*	*Name*	*Description*
117	DM	SEV_UDS_CLEAR_DTC_FAILED	Clearing DTC information has been requested by SID 0x14 ClearDiagnosticInformation, but failed.
118	DM	SEV_UDS_CONTROL_DTC_SETTING_SUCCESSFUL	The control of a DTC setting has been requested by service SID 0x85 Control DTCSetting successfully.
119	DM	SEV_UDS_CONTROL_DTC_SETTING_FAILED	Control of DTC setting has been requested by service SID 0x85 ControlDTCSetting, but failed.
120	DM	SEV_UDS_ECU_RESET_SUCCESSFUL	ECU has been reset by SID 0x11 ECUReset.
121	DM	SEV_UDS_ECU_RESET_FAILED	ECU Reset has been requested by SID 0x11 ECUReset, but failed.
122	DM	SEV_UDS_ROUTINE_CONTROL_SUCCESSFUL	The control of a routine has been requested by service SID 0x31 RoutineControl successfully.
123	DM	SEV_UDS_ROUTINE_CONTROL_FAILED	The control of a routine has been requested by service SID 0x31 RoutineControl, but failed.
127	DM	SEV_DOIP_HEADER_CHECK_FAILED	The DoIP Header Handler rejected a request (routing or diagnostic message).
128	DM	SEV_DOIP_ROUTING_ACTIVATION_CHECK_FAILED	A routing request was rejected by the routing handler.
129	DM	SEV_DOIP_ROUTING_ACTIVATION_SUCCESS	A routing request was successful.
130	DM	SEV_DOIP_DIAG_MESSAGE_CHECK_FAILED	A diagnostic message request was rejected by the diagnostic message handler.
133	DM	SEV_ACCESS_CONTROL_DM_IAM_ACCESS_DENIED	Access of an application to a resource provided by DM was denied.
127	DoIP	SEV_DOIP_HEADER_CHECK_FAILED	The DoIP Header Handler rejected a request (routing or diagnostic message).
128	DoIP	SEV_DOIP_ROUTING_ACTIVATION_CHECK_FAILED	A routing request was rejected by the routing handler.
129	DoIP	SEV_DOIP_ROUTING_ACTIVATION_SUCCESS	A routing request was successful.
130	DoIP	SEV_DOIP_DIAG_MESSAGE_CHECK_FAILED	A diagnostic message request was rejected by the diagnostic message handler.
93	UCM	SEV_SW_UPDATE_FAILED	A SW update operation was requested, but it was not successful.
94	UCM	SEV_SW_UPDATE_SUCCESS	A SW update operation was executed successfully.
99	EM	SEV_EXEC_SW_COMPONENT_INTEGRITY_CHECK_FAILED	The integrity check of a SW component has failed.
65	PHM	SEV_ACCESS_CONTROL_PHM_IAM_ACCESS_DENIED	Access of an application to a resource provided by Platform Health Management was denied.
99	Crypto	SEV_EXEC_SW_COMPONENT_INTEGRITY_CHECK_FAILED	The integrity check of a SW component has failed.
5	CRYPT	SEV_CERT_CHAIN_VERIFICATION_FAILED	The verification of a certificate against a certificate chain was not successful.
95	CRYPT	SEV_CERT_INSTALL	Attempt to install a new certificate.
96	CRYPT	SEV_CERT_UPDATE	Attempt to update a certificate.
97	CRYPT	SEV_CERT_DELETE	Attempt to delete a certificate.
134	CRYPT	SEV_ACCESS_CONTROL_CRYPTO_IAM_ACCESS_DENIED	Access of an application to a resource provided by Cryptography was denied.

▽

△

ID	Owner	Name	Description
137	SM	SEV_ACCESS_CONTROL_SM_IAM_ACCESS_DENIED	Access of an application to a resource provided by State Management was denied.

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 [3].

5.1 Communication SEvs

5.1.1 TLS

[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	1	
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
TLSVersion	uint16	Version as defined in RFC5246, RFC8446 - 0x0303 for TLS Version 1.2 - 0x0304 for TLS 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_TcpIp_00395]

SEV Name	***SEV_TLS_CONNECTION_ESTABLISHED***	
ID	91	
Description	A TLS connection was successfully established.	
Context Data Version	1	
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
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_TcpIp_00396]

SEV Name	***SEV_TLS_CONNECTION_CLOSED***	
ID	92	
Description	A TLS connection was closed normally.	
Context Data Version	1	
Context Data	***Data Type***	***Allowed Values***

ReasonForClosure	uint8	close_notify(0)
		user_canceled(90)

TLSVersion	uint16	Version as defined in RFC5246, RFC8446 - 0x0303 for TLS Version 1.2 - 0x0304 for TLS 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	

5.1.2 MACsec

[CP_SWS_Mka_00309]

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]

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]

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]

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]

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]	

5.1.3 SecOC

[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_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	

5.1.4 Firewall

[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.

[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

▽

△

SEV Name	***SEV_FW_PACKET_BLOCKED_TCP_MISMATCH***	
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

▽

△

SEV Name	SEV_FW_PACKET_BLOCKED_DOIP_MISMATCH	
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
	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]	

[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	

5.1.5 CAN

[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***
ControllerId	uint8	
ErrorCounterThreshold	uint8	TxErrorCounter > 127 AND RxErrorCounter > 127 (0x00) TxErrorCounter > 127 AND RxErrorCounter < 127 (0x01) RxErrorCounter > 127 AND TxErrorCounter < 127 (0x02)

[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	

5.1.6 Ethernet

[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_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

▽

△

SEV Name	***SEV_ETH_DROP_VLAN_DOUBLE_TAG***	
EthernetFrame	uint8 [54]	EthernetFrame, truncated to the first EthIfSEvEthernetFrameMaxLength 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_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 EthIfSEvEthernetFrameMaxLength 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_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 EthIfSEvEthernetFrameMaxLength 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.

5.1.7 TCP/IP

[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***

▽

△

SEV Name	***SEV_ARP_IP_ADDR_CONFLICT***	
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_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_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_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

▽

△

SEV Name	***SEV_IPV4_DROP_INV_DEST_ADDR***	
	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_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 Signal-based communication

[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	

5.1.9 Time Synchronization

[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_TS_14214]

[SWS_EthTSyn_92000]

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_TS_14215]

[SWS_EthTSyn_92001]

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_TS_14216]

[SWS_EthTSyn_92002]

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_TS_14217]

[SWS_EthTSyn_92003]

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	

[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	

5.2 Cryptography SEvs

5.2.1 Certificates

[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***
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***
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 KeyMSEvCertificateMaxLength 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 KeyMSEvCertificateMaxLength 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

[SWS_DoIP_00511]

[SWS_DM_02135]

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_DoIP_00512]

[SWS_DM_02137]

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_DoIP_00513]

[SWS_DM_02139]

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_DoIP_00514]

[SWS_DM_02141]

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

5.3.2 UDS

[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***

▽

△

SEV Name	***SEV_UDS_AUTHENTICATION_FAILED***	
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_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	1	
Context Data	***Data Type***	***Allowed Values***
SID	uint8	
MemoryAddress	uint32	
MemorySize	uint32	
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	1	
Context Data	*Data Type*	*Allowed Values*
SID	uint8	
MemoryAddress	uint32	
MemorySize	uint32	
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	
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
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.

▽

△

SEV Name	***SEV_UDS_CLEAR_DTC_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***

▽

△

SEV Name	*SEV_UDS_ECU_RESET_SUCCESSFUL*	
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 InputOutputControlByIdentifier 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 InputOutputControlByIdentifier, but failed.	
Context Data Version	1	
Context Data	*Data Type*	*Allowed Values*
DID	uint16	
inputOutputControlParameter	uint8	
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	1	
Context Data	*Data Type*	*Allowed Values*
MemoryAddress	uint32	
MemorySize	uint32	
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	1	
Context Data	*Data Type*	*Allowed Values*
MemoryAddress	uint32	
MemorySize	uint32	
ClientSourceAddress	uint16	

▽

△

SEV Name	***SEV_UDS_WRITE_MEMORY_FAILED***	
NegativeResponseCode	uint8	

5.4 Identity and Access Management SEvs

[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_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_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_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	

[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_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	

[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	

5.5 Secure Boot SEvs

[SWS_EM_02589]

[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)

5.6 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	uint16 [128, encoding UTF-8]	
ReceivedSwVersion	uint16 [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	uint16 [128, encoding UTF-8]	
ReceivedSwVersion	uint16 [32, encoding UTF-8]	