Document Title	Specification of Secure Onboard Communication
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	654

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

Document Change History

Date	Release	Changed by	Change Description
2019-11-28	R19-11	AUTOSAR Release Management	• Added option to send default authentication information • Added an authentic PDU length header • Added new options to override the verification status • Minor corrections / clarifications / editorial changes; For details please refer to the Change Documentation • Changed Document Status from Final to published
2018-10-31	4.4.0	AUTOSAR Release Management	• Handle Dynamic length PDUs • Added option to send wrong Authentication Information • Provide failed verification status to application. • Minor corrections / clarifications / editorial changes; For details please refer to the Change Documentation.
2017-12-08	4.3.1	AUTOSAR Release Management	• Clarify new authentication data layout with optional parameters. • Clarified the details for SW-C Freshness Value Manager (Section 11). • Minor corrections / clarifications / editorial changes; For details please refer to the Change Documentation.

Document Change History			
Date	**Release**	**Changed by**	**Change Description**
2016-11-30	4.3.0	AUTOSAR Release Management	• Handle freshness in external freshness manager • New feature to send authenticator in an additional message • Secured diagnostic communication • Increase minimum value of parameter AuthInfoTxLength to 1 • Changed the type of the parameter keyID of the interface SecOC_AssociateKey() to uint16
2015-07-31	4.2.2	AUTOSAR Release Management	• Minor corrections / clarifications / editorial changes; For details please refer to the Change Documentation
2014-10-31	4.2.1	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 and functional overview 8
2 Acronyms, abbreviations and definitions 10
2.1 Acronyms and abbreviations 10
2.2 Definitions 10
3 Related documentation 12
3.1 Input documents 12
3.2 Related standards and norms 13
3.3 Related specification 13
4 Constraints and assumptions 14
4.1 Applicability to car domains 14
5 Dependencies to other modules 15
5.1 Dependencies to PduR 15
5.2 Dependencies to CSM 15
5.3 Dependencies to the RTE 15
6 Requirements traceability 16
7 Functional specification 28
7.1 Specification of the security solution 28
7.1.1 Basic entities of the security solution 29
7.1.2 Authentication of I-PDUs 38
7.1.3 Verification of I-PDUs 39
7.1.4 Adaptation in case of asymmetric approach 42
7.2 Relationship to PduR 42
7.3 Initialization 43
7.4 Authentication of outgoing PDUs 44
7.4.1 Authentication during direct transmission 46
7.4.2 Authentication during triggered transmission 47
7.4.3 Authentication during transport protocol transmission 49
7.4.4 Error handling and cancelation of transmission 51
7.5 Verification of incoming PDUs 52
7.5.1 Verification during bus interface reception 55
7.5.2 Verification during transport protocol reception 56
7.5.3 Skipping Authentication for Secured I-PDUs at SecOC 58
7.5.4 Error handling and discarding of reception 58
7.6 Gateway functionality 60
7.7 Multicore Distribution 60
7.8 Error Classification 60
7.8.1 Development Errors 60
7.8.2 Runtime Errors 61
7.8.3 Transient Faults 61
7.8.4 Production Errors 61
7.8.5 Extended Production Errors 61
7.9 Error detection 61

7.10 Error notification 61
7.11 Security Profiles 62
7.11.1 Secured area within a Pdu 62
7.11.2 Overview of security profiles 63
7.11.3 SecOC Profile 1 (or 24Bit-CMAC-8Bit-FV) 63
7.11.4 SecOC Profile 2 (or 24Bit-CMAC-No-FV) 64
7.11.5 SecOC Profile 3 (or JASPAR) 64
8 API specification 66
8.1 Imported types 66
8.2 Type definitions 66
8.2.1 SecOC_ConfigType 66
8.2.2 SecOC_StateType 67
8.3 Function definitions 67
8.3.1 SecOC_Init 67
8.3.2 SecOC_DeInit 68
8.3.3 SecOC_GetVersionInfo 68
8.3.4 SecOC_IfTransmit 69
8.3.5 SecOC_TpTransmit 70
8.3.6 SecOC_IfCancelTransmit 70
8.3.7 SecOC_TpCancelTransmit 71
8.3.8 SecOC_TpCancelReceive 71
8.3.9 Optional Interfaces 72
8.4 Call-back notifications 74
8.4.1 SecOC_RxIndication 74
8.4.2 SecOC_TpRxIndication 75
8.4.3 SecOC_TxConfirmation 75
8.4.4 SecOC_TpTxConfirmation 76
8.4.5 SecOC_TriggerTransmit 77
8.4.6 SecOC_CopyRxData 78
8.4.7 SecOC_CopyTxData 78
8.4.8 SecOC_StartOfReception 80
8.4.9 CSM callback interfaces 81
8.5 Callout Definitions 81
8.5.1 SecOC_GetRxFreshness 81
8.5.2 SecOC_GetRxFreshnessAuthData 82
8.5.3 SecOC_GetTxFreshness 83
8.5.4 SecOC_GetTxFreshnessTruncData 84
8.5.5 SecOC_SPduTxConfirmation 85
8.6 Scheduled functions 85
8.6.1 SecOC_MainFunctionRx 85
8.6.2 SecOC_MainFunctionTx 86
8.7 Expected Interfaces 87
8.7.1 Mandatory Interfaces 87
8.7.2 Optional Interfaces 88
8.7.3 Configurable Interfaces 88
8.8 Service Interfaces 90
8.8.1 Overview 90
8.8.2 Sender Receiver Interfaces 90
8.8.3 Client Server Interfaces 91

8.8.4 Ports 98
8.8.5 Implementation Data Types 99
9 Sequence diagrams 102
9.1 Authentication of outgoing PDUs 103
9.1.1 Authentication during direct transmission 103
9.1.2 Authentication during triggered transmission 104
9.1.3 Authentication during transport protocol transmission 105
9.1.4 Authentication with upper layer transport protocol 107
9.2 Verification of incoming PDUs 108
9.2.1 Verification during direct reception 108
9.2.2 Verification during transport protocol reception 109
9.2.3 Verification with upper layer transport protocol 110
9.3 Re-authentication Gateway 111
9.4 Freshness Handling 112
10 Configuration specification 113
10.1 Containers and configuration parameters 113
10.1.1 SecOC 116
10.1.2 SecOCGeneral 118
10.1.3 SecOCSameBufferPduCollection 122
10.1.4 SecOCRxPduProcessing 123
10.1.5 SecOCRxSecuredPduLayer 128
10.1.6 SecOCRxSecuredPdu 128
10.1.7 SecOCRxAuthenticPduLayer 129
10.1.8 SecOCRxSecuredPduCollection 130
10.1.9 SecOCRxCryptographicPdu 131
10.1.10 SecOCRxAuthenticPdu 132
10.1.11 SecOCTxPduProcessing 133
10.1.12 SecOCTxAuthenticPduLayer 136
10.1.13 SecOCTxSecuredPduLayer 137
10.1.14 SecOCTxSecuredPdu 138
10.1.15 SecOCTxSecuredPduCollection 139
10.1.16 SecOCTxAuthenticPdu 139
10.1.17 SecOCTxCryptographicPdu 140
10.1.18 SecOCUseMessageLink 141
10.1.19 SecOCTxPduSecuredArea 142
10.1.20 SecOCRxPduSecuredArea 142
10.2 Published Information 143
11 Annex A: Application hints for the development of SW-C Freshness Value Manager 144
11.1 Overview of freshness value construction 144
11.2 Freshness Value Based on Single Freshness Counter 144
11.3 Freshness Value Based on Single Freshness Timestamp 145
11.4 Freshness Value Based on Multiple Freshness Counters 147
11.4.1 Definition of Freshness Value 149
11.4.2 Synchronization Message Format 153
11.4.3 Processing of FV Management Master 153
11.4.4 Processing of Slave ECUs 154

A Not applicable requirements..... 161

1 Introduction and functional overview

This specification is the AUTOSAR Secure Onboard Communication (SecOC) module Software Specification. It is based on AUTOSAR SecOC[5] and specifies how the requirements of the AUTOSAR SecOC SRS shall be realized. It describes the basic security features, the functionality and the API of the AUTOSAR SecOC module.

The SecOC module aims for resource-efficient and practicable authentication mechanisms for critical data on the level of PDUs. The authentication mechanisms shall be seamlessly integrated with the current AUTOSAR communication systems. The impact with respect to resource consumption should be as small as possible in order to allow protection as add-on for legacy systems. The specification is based on the assumption that mainly symmetric authentication approaches with message authentication codes (MACs) are used. They achieve the same level of security with much smaller keys than asymmetric approaches and can be implemented compactly and efficiently in software and in hardware. However, the specification provides the necessary level of abstraction so that both, symmetric approaches as well as asymmetric authentication approaches can be used.

The SecOC module integrates on the level of the AUTOSAR PduR. **Figure 1** shows the integration of the SecOC module as part of the Autosar communication stack.

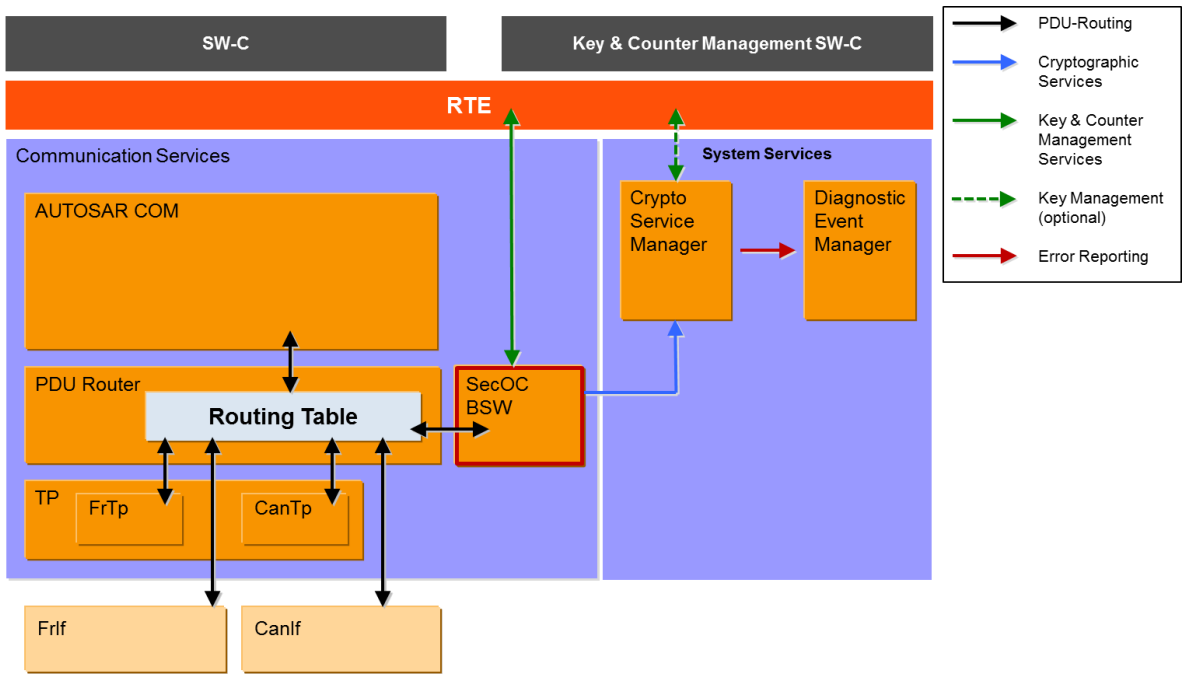

Figure 1: Integration of the SecOC BSW

In this setting,PduR is responsible to route incoming and outgoing security related I-PDUs to the SecOC module. The SecOC module shall then add or process the security relevant information and shall propagate the results in the form of an I-PDU back to the PduR. PduR is then responsible to further route the I-PDUs.Moreover, the SecOC module makes use of the cryptographic services provided by the CSM and interacts with the Rte to allow key and counter management. The SecOC

module shall support all kind of communication paradigms and principles that are supported by PduR, especially Multicast communications, Transport Protocols and the PduR Gateway. The following sections provide a detailed specification of SecOC interfaces, functionality and configuration.

2 Acronyms, abbreviations and definitions

2.1 Acronyms and abbreviations

Abbreviation / Acronym:	***Description:***
CSM	The AUTOSAR Crypto Service Manager
SecOC	Secure Onboard Communication
MAC	Message Authentication Code
FV	Freshness Value
FM	Freshness Manager

2.2 Definitions

For this document the definitions of data integrity, authentication, entity authentication, data origin, message authentication and transaction authentication from [14] are used:

Term:	***Description:***
Authentic I-PDU	An Authentic I-PDU is an arbitrary AUTOSAR I-PDU the content of which is secured during network transmission by means of the Secured I-PDU. The secured content comprises the complete I-PDU or a part of the I-PDU.
Authentication	Authentication is a service related to identification. This function applies to both entities and information itself. Two parties entering into a communication should identify each other. Information delivered over a channel should be authenticated as to origin, date of origin, data content, time sent, etc. For these reasons, this aspect of cryptography is usually subdivided into two major classes: entity authentication and data origin authentication. Data origin authentication implicitly provides data integrity (for if a message is modified, the source has changed).
Authentication Information	The Authentication Information consists of a Freshness Value (or a part thereof) and an Authenticator (or a part thereof). Authentication Information are the additional pieces of information that are added by SecOC to realize the Secured I-PDU
Authenticator	Authenticator is data that is used to provide message authentication. In general, the term Message Authentication Code (MAC) is used for symmetric approaches while the term Signature or Digital Signature refers to asymmetric approaches having different properties and constraints.
Data integrity	Data integrity is the property whereby data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source. To assure data integrity, one should have the ability to detect data manipulation by unauthorized parties. Data manipulation includes such things as insertion,

	deletion, and substitution.
Data origin authentication	Data origin authentication is a type of authentication whereby a party is corroborated as the (original) source of specified data created at some (typically unspecified) time in the past. By definition, data origin authentication includes data integrity.
Distinction unilateral/ bilateral authentication	In unilateral authentication, one side proves identity. The requesting side is not even authenticated to the extent of proving that it is allowed to request authentication. In bilateral authentication, the requester is also authenticated at least (see below) to prove the privilege of requesting. There is an efficient and more secure way to authenticate both endpoints, based on the bilateral authentication described above. Along with the authentication (in the second message) requested initially by the receiver (in the first message), the sender also requests an authentication. The receiver sends a third message providing the authentication requested by the sender. This is only three messages (in contrast to four with two unilateral messages).
Entity authentication	Entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired). Note: Entity authentication means to prove presence and operational readiness of a communication endpoint. This is for example often done by proving access to a cryptographic key and knowledge of a secret.It is necessary to do this without disclosing either key or secret.Entity authentication can be used to prevent record-and-replay attacks. Freshness of messages only complicates them by the need to record a lifetime and corrupt either senders or receivers (real-time) clock.Entity authentication is triggered by the receiver, i.e. the one to be convinced, while the sender has to react by convincing. Record and replay attacks on entity authentication are usually prevented by allowing the receiver some control over the authentication process.In order to prevent the receiver from using this control for steering the sender to malicious purposes or from determining a key or a secret ("oracle attack"), the sender can add more randomness.If not only access to a key (implying membership to a privileged group) but also individuality is to be proven, the sender additionally adds and authenticates its unique identification.
Message authentication	Message authentication is a term used analogously with data origin authentication. It provides data origin authentication with respect to the original message source (and data integrity, but no uniqueness and timeliness guarantees).
Secured I-PDU	A Secured I-PDU is an AUTOSAR I-PDU that contains Payload of an Authentic I-PDU supplemented by additional Authentication Information.
Transaction authentication	Transaction authentication denotes message authentication augmented to additionally provide uniqueness and timeliness guarantees on data (thus preventing undetectable message replay).

3 Related documentation

3.1 Input documents

[1] AUTOSAR Layered Software Architecture
AUTOSAR_EXP_LayeredSoftwareArchitecture.pdf

[2] AUTOSAR General Requirements on Basic Software Modules
AUTOSAR_SRS_BSWGeneral.pdf

[3] AUTOSAR General Specification for Basic Software Modules
AUTOSAR_SWS_BSWGeneral.pdf

[4] Specification of Communication
AUTOSAR_SWS_COM - Specification of Communication

[5] AUTOSAR SecOC Software Requirements Specification
AUTOSAR_SRS_SecureOnboardCommunication.pdf

[6] Specification of I-PDU Multiplexer
AUTOSAR_SWS_I-PDUMultiplexer.pdf

[7] Specification of PDU Router
AUTOSAR_SWS_PduRouter.pdf

[8] Specification of Crypt Service Manager
AUTOSAR_SWS_CryptoServiceManager.pdf

[9] System Template,
https://svn3.autosar.org/repos2/work/24_Sources/branches/R4.0/TPS_SystemTemplate_063/AUTOSAR_TPS_SystemTemplate.pdf

[10] Software Component Template,
https://svn3.autosar.org/repos2/work/24_Sources/branches/R4.0/TPS_SoftwareComponentTemplate_062/AUTOSAR_TPS_SoftwareComponentTemplate.pdf

[11] Koscher et al: Experimental Security Analysis of a Modern Automobile, 2010 IEEE Symposium on Security and Privacy

[12] Checkoway et al: Comprehensive Experimental Analyses of Automotive Attack Surfaces, USENIX Security 2011

[13] Auguste Kerckhoffs, ‘La cryptographie militaire’, Journal des sciences militaires, vol. IX, pp. 5–38, Jan. 1883, pp. 161–191, Feb. 1883.

[14] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1996.

[15] Danny Dolev and Andrew C. Yao: On the security of public key protocols, In Foundations of Computer Science, SFCS 1981

[16] M. Dworkin: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, U.S. Department of Commerce, Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, NIST Special Publication 800-38B, 2005

3.2 Related standards and norms

[17] IEC 7498-1 The Basic Model, IEC Norm, 1994

[18] National Institute of Standards and Technology (NIST): FIPS-180-4, Secure Hash Standard (SHS), March 2012, available electronically at http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[19] FIPS Pub 197: Advanced Encryption Standard (AES), U.S. Department of Commerce, Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Federal Information Processing Standards Publication, 2001, electronically available at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

3.3 Related specification

AUTOSAR provides a General Specification on Basic Software (SWS BSW General) [3], which is also valid for SecOC module

Thus, the SWS BSW General specification[3] shall be considered as an additional set of requirements for the AUTOSAR SecOC module.

4 Constraints and assumptions

This document is applicable for AUTOSAR release 4.3.

4.1 Applicability to car domains

The SecOC module is used in all ECUs where secure communication is necessary.

The SecOC module has not been specified to work with MOST and LIN communication networks. With MOST not being specifically supported,the applicability to multimedia and telematic car domains may be limited.

5 Dependencies to other modules

This chapter lists all the features from other modules that are used by the AUTOSAR SecOC module and functionalities that are provided by the AUTOSAR SecOC module to other modules. Because the SecOC module deals with I-PDUs that are either sourced or sunk by other modules, care should be taken that shared configuration items are consistent between the modules.

5.1 Dependencies to PduR

The SecOC module depends on the API and capabilities of the PduR. It provides the upper and lower layer API functions required by the PDU Router, namely

- the API of the communication interface modules,
- the API of the Transport Protocol Modules,
- the API of the upper layer modules which use transport protocol modules,
- the API of the upper layer modules which process I-PDUs originating from communication interface modules.

To serve the PduR with the results of the security processing, the SecOC module requires the respective API function of the PduR.

5.2 Dependencies to CSM

The SecOC module depends on cryptographic algorithms that are provided in AUTOSAR by the CSM module. The SecOC module requires API functions to generate and verify Cryptographic Signatures or Message Authentication Codes, namely

- the MAC-generate interface (Csm_MacGenerate),
- the MAC-verify interface (Csm_MacVerify),
- the Signature-generate interface (Csm_SignatureGenerate),
- the Signature-verify interface (Csm_SignatureVerify),

5.3 Dependencies to the RTE

The SecOC module provides an API with management functions. This API contains the following API functions that are provided as Service Interfaces by the RTE.

- SecOC_VerificationStatus
- SecOC_VerifyStatusOverride.

The API functions are specified in more detail in Section 0.

The Rte includes the BSW-Scheduler. The SecOC module relies on the BSW-scheduler calling the functions SecOC_MainFunctionRx and SecOC_MainFunctionTx at a period as configured in SecOCMainFunctionPeriodRx and SecOCMainFunctionPeriodTx.

6 Requirements traceability

The following table references the requirements specified in[3] and [5] and links to the fulfillment of these.

Requirement	Description	Satisfied by
SRS_BSW_00003	All software modules shall provide version and identification information	SWS_SecOC_00107
SRS_BSW_00004	All Basic SW Modules shall perform a pre-processor check of the versions of all imported include files	SWS_SecOC_00999
SRS_BSW_00005	Modules of the µC Abstraction Layer (MCAL) may not have hard coded horizontal interfaces	SWS_SecOC_00999
SRS_BSW_00006	The source code of software modules above the µC Abstraction Layer (MCAL) shall not be processor and compiler dependent.	SWS_SecOC_00999
SRS_BSW_00007	All Basic SW Modules written in C language shall conform to the MISRA C 2012 Standard.	SWS_SecOC_00999
SRS_BSW_00009	All Basic SW Modules shall be documented according to a common standard.	SWS_SecOC_00999
SRS_BSW_00010	The memory consumption of all Basic SW Modules shall be documented for a defined configuration for all supported platforms.	SWS_SecOC_00999
SRS_BSW_00101	The Basic Software Module shall be able to initialize variables and hardware in a separate initialization function	SWS_SecOC_00106
SRS_BSW_00158	-	SWS_SecOC_00999
SRS_BSW_00160	Configuration files of AUTOSAR Basic SW module shall be readable for human beings	SWS_SecOC_00999
SRS_BSW_00161	The AUTOSAR Basic Software shall provide a microcontroller abstraction layer which provides a standardized interface to higher software layers	SWS_SecOC_00999
SRS_BSW_00162	The AUTOSAR Basic Software shall provide a hardware abstraction layer	SWS_SecOC_00999
SRS_BSW_00164	The Implementation of interrupt	SWS_SecOC_00999

	service routines shall be done by the Operating System, complex drivers or modules	
SRS_BSW_00167	All AUTOSAR Basic Software Modules shall provide configuration rules and constraints to enable plausibility checks	SWS_SecOC_00999
SRS_BSW_00168	SW components shall be tested by a function defined in a common API in the Basis-SW	SWS_SecOC_00999
SRS_BSW_00170	The AUTOSAR SW Components shall provide information about their dependency from faults, signal qualities, driver demands	SWS_SecOC_00999
SRS_BSW_00171	Optional functionality of a Basic-SW component that is not required in the ECU shall be configurable at pre-compile-time	SWS_SecOC_00153
SRS_BSW_00172	The scheduling strategy that is built inside the Basic Software Modules shall be compatible with the strategy used in the system	SWS_SecOC_00999
SRS_BSW_00300	All AUTOSAR Basic Software Modules shall be identified by an unambiguous name	SWS_SecOC_00999
SRS_BSW_00301	All AUTOSAR Basic Software Modules shall only import the necessary information	SWS_SecOC_00103
SRS_BSW_00302	All AUTOSAR Basic Software Modules shall only export information needed by other modules	SWS_SecOC_00999
SRS_BSW_00304	All AUTOSAR Basic Software Modules shall use the following data types instead of native C data types	SWS_SecOC_00999
SRS_BSW_00305	Data types naming convention	SWS_SecOC_00999
SRS_BSW_00306	AUTOSAR Basic Software Modules shall be compiler and platform independent	SWS_SecOC_00999
SRS_BSW_00307	Global variables naming convention	SWS_SecOC_00999
SRS_BSW_00308	AUTOSAR Basic Software Modules shall not define global data in their header files, but in the C file	SWS_SecOC_00999
SRS_BSW_00309	All AUTOSAR Basic Software	SWS_SecOC_00999

	Modules shall indicate all global data with read-only purposes by explicitly assigning the const keyword	
SRS_BSW_00310	API naming convention	SWS_SecOC_00999
SRS_BSW_00312	Shared code shall be reentrant	SWS_SecOC_00999
SRS_BSW_00314	All internal driver modules shall separate the interrupt frame definition from the service routine	SWS_SecOC_00999
SRS_BSW_00318	Each AUTOSAR Basic Software Module file shall provide version numbers in the header file	SWS_SecOC_00999
SRS_BSW_00321	The version numbers of AUTOSAR Basic Software Modules shall be enumerated according specific rules	SWS_SecOC_00999
SRS_BSW_00323	All AUTOSAR Basic Software Modules shall check passed API parameters for validity	SWS_SecOC_00106, SWS_SecOC_00107, SWS_SecOC_00112, SWS_SecOC_00113, SWS_SecOC_00122, SWS_SecOC_00124, SWS_SecOC_00125, SWS_SecOC_00126, SWS_SecOC_00127, SWS_SecOC_00128, SWS_SecOC_00129, SWS_SecOC_00130, SWS_SecOC_00152, SWS_SecOC_00157, SWS_SecOC_00161, SWS_SecOC_91008, SWS_SecOC_91009
SRS_BSW_00325	The runtime of interrupt service routines and functions that are running in interrupt context shall be kept short	SWS_SecOC_00999
SRS_BSW_00327	Error values naming convention	SWS_SecOC_00999
SRS_BSW_00328	All AUTOSAR Basic Software Modules shall avoid the duplication of code	SWS_SecOC_00999
SRS_BSW_00330	It shall be allowed to use macros instead of functions where source code is used and runtime is critical	SWS_SecOC_00999
SRS_BSW_00331	All Basic Software Modules shall strictly separate error and status information	SWS_SecOC_00999
SRS_BSW_00333	For each callback function it shall be specified if it is called from interrupt context or not	SWS_SecOC_00999
SRS_BSW_00334	All Basic Software Modules shall provide an XML file that contains the meta data	SWS_SecOC_00999
SRS_BSW_00335	Status values naming convention	SWS_SecOC_00999
SRS_BSW_00336	Basic SW module shall be able	SWS_SecOC_00999

	to shutdown	
SRS_BSW_00337	Classification of development errors	SWS_SecOC_00101, SWS_SecOC_00102, SWS_SecOC_00114, SWS_SecOC_00164, SWS_SecOC_00166
SRS_BSW_00339	Reporting of production relevant error status	SWS_SecOC_00999
SRS_BSW_00341	Module documentation shall contains all needed informations	SWS_SecOC_00999
SRS_BSW_00342	It shall be possible to create an AUTOSAR ECU out of modules provided as source code and modules provided as object code, even mixed	SWS_SecOC_00999
SRS_BSW_00343	The unit of time for specification and configuration of Basic SW modules shall be preferably in physical time unit	SWS_SecOC_00999
SRS_BSW_00346	All AUTOSAR Basic Software Modules shall provide at least a basic set of module files	SWS_SecOC_00999
SRS_BSW_00347	A Naming seperation of different instances of BSW drivers shall be in place	SWS_SecOC_00999
SRS_BSW_00350	All AUTOSAR Basic Software Modules shall allow the enabling/disabling of detection and reporting of development errors.	SWS_SecOC_00102, SWS_SecOC_00164, SWS_SecOC_00166
SRS_BSW_00357	For success/failure of an API call a standard return type shall be defined	SWS_SecOC_00112, SWS_SecOC_00113, SWS_SecOC_00122, SWS_SecOC_00127, SWS_SecOC_00128, SWS_SecOC_00129, SWS_SecOC_00130, SWS_SecOC_91008, SWS_SecOC_91009
SRS_BSW_00358	The return type of init() functions implemented by AUTOSAR Basic Software Modules shall be void	SWS_SecOC_00106
SRS_BSW_00359	All AUTOSAR Basic Software Modules callback functions shall avoid return types other than void if possible	SWS_SecOC_00106, SWS_SecOC_00107, SWS_SecOC_00119, SWS_SecOC_00124, SWS_SecOC_00125, SWS_SecOC_00126, SWS_SecOC_00152, SWS_SecOC_00161
SRS_BSW_00360	AUTOSAR Basic Software Modules callback functions are allowed to have parameters	SWS_SecOC_00999
SRS_BSW_00361	All mappings of not standardized keywords of compiler specific scope shall be placed and organized in a compiler specific type and keyword header	SWS_SecOC_00999
SRS_BSW_00369	All AUTOSAR Basic Software	SWS_SecOC_00107, SWS_SecOC_00112,

	Modules shall not return specific development error codes via the API	SWS_SecOC_91008
SRS_BSW_00371	The passing of function pointers as API parameter is forbidden for all AUTOSAR Basic Software Modules	SWS_SecOC_00999
SRS_BSW_00373	The main processing function of each AUTOSAR Basic Software Module shall be named according the defined convention	SWS_SecOC_00171, SWS_SecOC_00176
SRS_BSW_00374	All Basic Software Modules shall provide a readable module vendor identification	SWS_SecOC_00999
SRS_BSW_00375	Basic Software Modules shall report wake-up reasons	SWS_SecOC_00999
SRS_BSW_00377	A Basic Software Module can return a module specific types	SWS_SecOC_00999
SRS_BSW_00378	AUTOSAR shall provide a boolean type	SWS_SecOC_00999
SRS_BSW_00379	All software modules shall provide a module identifier in the header file and in the module XML description file.	SWS_SecOC_00999
SRS_BSW_00380	Configuration parameters being stored in memory shall be placed into separate c-files	SWS_SecOC_00999
SRS_BSW_00383	The Basic Software Module specifications shall specify which other configuration files from other modules they use at least in the description	SWS_SecOC_00999
SRS_BSW_00384	The Basic Software Module specifications shall specify at least in the description which other modules they require	SWS_SecOC_00137, SWS_SecOC_00138
SRS_BSW_00385	List possible error notifications	SWS_SecOC_00077, SWS_SecOC_00089, SWS_SecOC_00101, SWS_SecOC_00102, SWS_SecOC_00108, SWS_SecOC_00109, SWS_SecOC_00114, SWS_SecOC_00121, SWS_SecOC_00151, SWS_SecOC_00155, SWS_SecOC_00164, SWS_SecOC_00166, SWS_SecOC_00213, SWS_SecOC_00263, SWS_SecOC_00264, SWS_SecOC_00265
SRS_BSW_00386	The BSW shall specify the configuration for detecting an error	SWS_SecOC_00101, SWS_SecOC_00114
SRS_BSW_00388	Containers shall be used to group configuration parameters that are defined for the same object	SWS_SecOC_00999

SRS_BSW_00389	Containers shall have names	SWS_SecOC_00999
SRS_BSW_00390	Parameter content shall be unique within the module	SWS_SecOC_00999
SRS_BSW_00392	Parameters shall have a type	SWS_SecOC_00999
SRS_BSW_00393	Parameters shall have a range	SWS_SecOC_00999
SRS_BSW_00394	The Basic Software Module specifications shall specify the scope of the configuration parameters	SWS_SecOC_00999
SRS_BSW_00395	The Basic Software Module specifications shall list all configuration parameter dependencies	SWS_SecOC_00999
SRS_BSW_00396	The Basic Software Module specifications shall specify the supported configuration classes for changing values and multiplicities for each parameter/container	SWS_SecOC_00999
SRS_BSW_00397	The configuration parameters in pre-compile time are fixed before compilation starts	SWS_SecOC_00999
SRS_BSW_00398	The link-time configuration is achieved on object code basis in the stage after compiling and before linking	SWS_SecOC_00999
SRS_BSW_00399	Parameter-sets shall be located in a separate segment and shall be loaded after the code	SWS_SecOC_00999
SRS_BSW_00400	Parameter shall be selected from multiple sets of parameters after code has been loaded and started	SWS_SecOC_00999
SRS_BSW_00401	Documentation of multiple instances of configuration parameters shall be available	SWS_SecOC_00999
SRS_BSW_00402	Each module shall provide version information	SWS_SecOC_00107
SRS_BSW_00405	BSW Modules shall support multiple configuration sets	SWS_SecOC_00999
SRS_BSW_00406	A static status variable denoting if a BSW module is initialized shall be initialized with value 0 before any APIs of the BSW module is called	SWS_SecOC_00999
SRS_BSW_00407	Each BSW module shall provide a function to read out the version information of a dedicated module implementation	SWS_SecOC_00107

SRS_BSW_00408	All AUTOSAR Basic Software Modules configuration parameters shall be named according to a specific naming rule	SWS_SecOC_00999
SRS_BSW_00409	All production code error ID symbols are defined by the Dem module and shall be retrieved by the other BSW modules from Dem configuration	SWS_SecOC_00999
SRS_BSW_00410	Compiler switches shall have defined values	SWS_SecOC_00999
SRS_BSW_00411	All AUTOSAR Basic Software Modules shall apply a naming rule for enabling/disabling the existence of the API	SWS_SecOC_00999
SRS_BSW_00412	-	SWS_SecOC_00999
SRS_BSW_00413	An index-based accessing of the instances of BSW modules shall be done	SWS_SecOC_00999
SRS_BSW_00414	Init functions shall have a pointer to a configuration structure as single parameter	SWS_SecOC_00106
SRS_BSW_00416	The sequence of modules to be initialized shall be configurable	SWS_SecOC_00999
SRS_BSW_00417	Software which is not part of the SW-C shall report error events only after the DEM is fully operational.	SWS_SecOC_00999
SRS_BSW_00419	If a pre-compile time configuration parameter is implemented as "const" it should be placed into a separate c-file	SWS_SecOC_00999
SRS_BSW_00422	Pre-de-bouncing of error status information is done within the DEM	SWS_SecOC_00999
SRS_BSW_00423	BSW modules with AUTOSAR interfaces shall be describable with the means of the SW-C Template	SWS_SecOC_00999
SRS_BSW_00424	BSW module main processing functions shall not be allowed to enter a wait state	SWS_SecOC_00999
SRS_BSW_00425	The BSW module description template shall provide means to model the defined trigger conditions of schedulable objects	SWS_SecOC_00171, SWS_SecOC_00176
SRS_BSW_00426	BSW Modules shall ensure	SWS_SecOC_00110

	data consistency of data which is shared between BSW modules	
SRS_BSW_00427	ISR functions shall be defined and documented in the BSW module description template	SWS_SecOC_00999
SRS_BSW_00428	A BSW module shall state if its main processing function(s) has to be executed in a specific order or sequence	SWS_SecOC_00999
SRS_BSW_00429	Access to OS is restricted	SWS_SecOC_00999
SRS_BSW_00432	Modules should have separate main processing functions for read/receive and write/transmit data path	SWS_SecOC_00999
SRS_BSW_00433	Main processing functions are only allowed to be called from task bodies provided by the BSW Scheduler	SWS_SecOC_00999
SRS_BSW_00437	Memory mapping shall provide the possibility to define RAM segments which are not to be initialized during startup	SWS_SecOC_00999
SRS_BSW_00438	Configuration data shall be defined in a structure	SWS_SecOC_00999
SRS_BSW_00439	Enable BSW modules to handle interrupts	SWS_SecOC_00999
SRS_BSW_00440	The callback function invocation by the BSW module shall follow the signature provided by RTE to invoke servers via Rte_Call API	SWS_SecOC_00999
SRS_BSW_00441	Naming convention for type, macro and function	SWS_SecOC_00999
SRS_BSW_00447	Standardizing Include file structure of BSW Modules Implementing Autosar Service	SWS_SecOC_00999
SRS_BSW_00448	Module SWS shall not contain requirements from Other Modules	SWS_SecOC_00999
SRS_BSW_00449	BSW Service APIs used by Autosar Application Software shall return a Std_ReturnType	SWS_SecOC_00112, SWS_SecOC_00113, SWS_SecOC_00122, SWS_SecOC_00125, SWS_SecOC_00127, SWS_SecOC_00152, SWS_SecOC_91008, SWS_SecOC_91009
SRS_BSW_00450	A Main function of a un-initialized module shall return immediately	SWS_SecOC_00102
SRS_BSW_00451	Hardware registers shall be protected if concurrent access to these registers occur	SWS_SecOC_00999
SRS_BSW_00452	Classification of runtime errors	SWS_SecOC_00999

SRS_BSW_00453	BSW Modules shall be harmonized	SWS_SecOC_00999
SRS_BSW_00454	An alternative interface without a parameter of category DATA_REFERENCE shall be available.	SWS_SecOC_00999
SRS_BSW_00456	A Header file shall be defined in order to harmonize BSW Modules	SWS_SecOC_00999
SRS_BSW_00457	Callback functions of Application software components shall be invoked by the Basis SW	SWS_SecOC_00012
SRS_BSW_00458	Classification of production errors	SWS_SecOC_00999
SRS_BSW_00459	It shall be possible to concurrently execute a service offered by a BSW module in different partitions	SWS_SecOC_00999
SRS_BSW_00460	Reentrancy Levels	SWS_SecOC_00999
SRS_BSW_00461	Modules called by generic modules shall satisfy all interfaces requested by the generic module	SWS_SecOC_00999
SRS_BSW_00462	All Standardized Autosar Interfaces shall have unique requirement Id / number	SWS_SecOC_00999
SRS_BSW_00463	Naming convention of callout prototypes	SWS_SecOC_00999
SRS_BSW_00464	File names shall be considered case sensitive regardless of the filesystem in which they are used	SWS_SecOC_00999
SRS_BSW_00465	It shall not be allowed to name any two files so that they only differ by the cases of their letters	SWS_SecOC_00999
SRS_BSW_00466	Classification of extended production errors	SWS_SecOC_00999
SRS_BSW_00467	The init / deinit services shall only be called by BswM or EcuM	SWS_SecOC_00999
SRS_BSW_00469	Fault detection and healing of production errors and extended production errors	SWS_SecOC_00999
SRS_BSW_00470	Execution frequency of production error detection	SWS_SecOC_00999
SRS_BSW_00471	Do not cause dead-locks on detection of production errors - the ability to heal from previously detected production	SWS_SecOC_00999

	errors	
SRS_BSW_00472	Avoid detection of two production errors with the same root cause.	SWS_SecOC_00999
SRS_SecOC_00001	Selection of Authentic I-PDU	SWS_SecOC_00104
SRS_SECOC_00002	-	SWS_SecOC_91005
SRS_SecOC_00002	Range of verification retry by the receiver	SWS_SecOC_00047, SWS_SecOC_00094, SWS_SecOC_00232, SWS_SecOC_00233
SRS_SECOC_00003	-	SWS_SecOC_91001, SWS_SecOC_91002, SWS_SecOC_91003, SWS_SecOC_91004, SWS_SecOC_91005, SWS_SecOC_91006, SWS_SecOC_91007, SWS_SecOC_91012
SRS_SecOC_00003	Configuration of different security properties / requirements	SWS_SecOC_00012, SWS_SecOC_00104, SWS_SecOC_00190, SWS_SecOC_00191, SWS_SecOC_00192, SWS_SecOC_00193, SWS_SecOC_00194, SWS_SecOC_00230, SWS_SecOC_00231, SWS_SecOC_00232, SWS_SecOC_00244, SWS_SecOC_00245, SWS_SecOC_00246, SWS_SecOC_00247, SWS_SecOC_00249, SWS_SecOC_00250
SRS_SecOC_00005	Initialisation of security information	SWS_SecOC_00054, SWS_SecOC_00162, SWS_SecOC_00172, SWS_SecOC_00177, SWS_SecOC_00226, SWS_SecOC_00235
SRS_SECOC_00006	-	SWS_SecOC_91003, SWS_SecOC_91004
SRS_SecOC_00006	Creation of a Secured I-PDU from an Authentic I-PDU	SWS_SecOC_00011, SWS_SecOC_00031, SWS_SecOC_00033, SWS_SecOC_00034, SWS_SecOC_00035, SWS_SecOC_00036, SWS_SecOC_00037, SWS_SecOC_00040, SWS_SecOC_00042, SWS_SecOC_00046, SWS_SecOC_00057, SWS_SecOC_00058, SWS_SecOC_00106, SWS_SecOC_00146, SWS_SecOC_00157, SWS_SecOC_00161, SWS_SecOC_00219, SWS_SecOC_00230, SWS_SecOC_00231, SWS_SecOC_00243, SWS_SecOC_00261, SWS_SecOC_00262
SRS_SecOC_00007	Verification retry by the receiver	SWS_SecOC_00047, SWS_SecOC_00094, SWS_SecOC_00234, SWS_SecOC_00235, SWS_SecOC_00236, SWS_SecOC_00237, SWS_SecOC_00238, SWS_SecOC_00239, SWS_SecOC_00240, SWS_SecOC_00241, SWS_SecOC_00242, SWS_SecOC_00243
SRS_SecOC_00010	Communication security is available for all communication paradigms of AUTOSAR	SWS_SecOC_00060, SWS_SecOC_00061, SWS_SecOC_00062, SWS_SecOC_00063, SWS_SecOC_00064, SWS_SecOC_00065, SWS_SecOC_00066, SWS_SecOC_00067, SWS_SecOC_00068, SWS_SecOC_00069, SWS_SecOC_00070, SWS_SecOC_00071, SWS_SecOC_00072, SWS_SecOC_00073, SWS_SecOC_00074, SWS_SecOC_00075, SWS_SecOC_00078, SWS_SecOC_00079, SWS_SecOC_00080, SWS_SecOC_00081, SWS_SecOC_00082, SWS_SecOC_00083, SWS_SecOC_00084, SWS_SecOC_00085, SWS_SecOC_00086, SWS_SecOC_00088,

		SWS_SecOC_00150
SRS_SecOC_00012	Support of Automotive BUS Systems	SWS_SecOC_00060, SWS_SecOC_00061, SWS_SecOC_00062, SWS_SecOC_00063, SWS_SecOC_00064, SWS_SecOC_00065, SWS_SecOC_00066, SWS_SecOC_00067, SWS_SecOC_00068, SWS_SecOC_00069, SWS_SecOC_00070, SWS_SecOC_00071, SWS_SecOC_00072, SWS_SecOC_00073, SWS_SecOC_00074, SWS_SecOC_00075, SWS_SecOC_00078, SWS_SecOC_00079, SWS_SecOC_00080, SWS_SecOC_00081, SWS_SecOC_00082, SWS_SecOC_00083, SWS_SecOC_00084, SWS_SecOC_00085, SWS_SecOC_00086, SWS_SecOC_00088, SWS_SecOC_00113, SWS_SecOC_00124, SWS_SecOC_00125, SWS_SecOC_00126, SWS_SecOC_00127, SWS_SecOC_00128, SWS_SecOC_00129, SWS_SecOC_00130, SWS_SecOC_00150, SWS_SecOC_00152, SWS_SecOC_91009
SRS_SecOC_00013	Support for end-to-end and point-to-point protection	SWS_SecOC_00060, SWS_SecOC_00061, SWS_SecOC_00062, SWS_SecOC_00063, SWS_SecOC_00064, SWS_SecOC_00065, SWS_SecOC_00066, SWS_SecOC_00067, SWS_SecOC_00068, SWS_SecOC_00069, SWS_SecOC_00070, SWS_SecOC_00071, SWS_SecOC_00072, SWS_SecOC_00073, SWS_SecOC_00074, SWS_SecOC_00075, SWS_SecOC_00078, SWS_SecOC_00079, SWS_SecOC_00080, SWS_SecOC_00081, SWS_SecOC_00082, SWS_SecOC_00083, SWS_SecOC_00084, SWS_SecOC_00085, SWS_SecOC_00086, SWS_SecOC_00088, SWS_SecOC_00150
SRS_SecOC_00017	PDU security information override	SWS_SecOC_00119, SWS_SecOC_00122, SWS_SecOC_00142, SWS_SecOC_00991
SRS_SecOC_00020	Security operational information persistency	SWS_SecOC_00161
SRS_SECOC_00021	-	SWS_SecOC_91002, SWS_SecOC_91012
SRS_SecOC_00021	Transmitted PDU authentication failure handling	SWS_SecOC_00076, SWS_SecOC_00087, SWS_SecOC_00151, SWS_SecOC_00214, SWS_SecOC_00215, SWS_SecOC_00216, SWS_SecOC_00217, SWS_SecOC_00218, SWS_SecOC_00225, SWS_SecOC_00226, SWS_SecOC_00227, SWS_SecOC_00228, SWS_SecOC_00229, SWS_SecOC_91013
SRS_SECOC_00022	-	SWS_SecOC_91002, SWS_SecOC_91012
SRS_SecOC_00022	Received PDU verification failure handling	SWS_SecOC_00047, SWS_SecOC_00048, SWS_SecOC_00050, SWS_SecOC_00087, SWS_SecOC_00121, SWS_SecOC_00141, SWS_SecOC_00148, SWS_SecOC_00149, SWS_SecOC_00160, SWS_SecOC_00214, SWS_SecOC_00215, SWS_SecOC_00216, SWS_SecOC_00236, SWS_SecOC_00237, SWS_SecOC_00238, SWS_SecOC_00239, SWS_SecOC_00240, SWS_SecOC_00241,

		SWS_SecOC_00248, SWS_SecOC_00251
SRS_SecOC_00025	Authentication and verification processing time	SWS_SecOC_00173, SWS_SecOC_00174, SWS_SecOC_00175, SWS_SecOC_00178, SWS_SecOC_00179, SWS_SecOC_00180
SRS_SecOC_00026	Capability to transmit data and authentication information separately	SWS_SecOC_00201, SWS_SecOC_00202, SWS_SecOC_00203, SWS_SecOC_00204, SWS_SecOC_00205, SWS_SecOC_00206, SWS_SecOC_00207, SWS_SecOC_00208
SRS_SecOC_00028	Properly match up data and authentication information when verifying	SWS_SecOC_00203, SWS_SecOC_00209, SWS_SecOC_00210, SWS_SecOC_00211
SRS_SecOC_00029	Flexible freshness construction	SWS_SecOC_00219, SWS_SecOC_00220, SWS_SecOC_00221, SWS_SecOC_00222, SWS_SecOC_00223, SWS_SecOC_00224, SWS_SecOC_00225, SWS_SecOC_00226, SWS_SecOC_00227, SWS_SecOC_00228, SWS_SecOC_00229, SWS_SecOC_00230, SWS_SecOC_00231, SWS_SecOC_00232, SWS_SecOC_00233, SWS_SecOC_00234, SWS_SecOC_00235, SWS_SecOC_00236, SWS_SecOC_00237, SWS_SecOC_00238, SWS_SecOC_00239, SWS_SecOC_00240, SWS_SecOC_00241, SWS_SecOC_00242, SWS_SecOC_00243, SWS_SecOC_00244, SWS_SecOC_00245, SWS_SecOC_00246, SWS_SecOC_00247, SWS_SecOC_00248, SWS_SecOC_00249, SWS_SecOC_00250, SWS_SecOC_00251
SRS_SecOC_00032	Interaction decoupling between upper and lower layer modules	SWS_SecOC_00252, SWS_SecOC_00255
SWS_BSW_00242	Access to Meta Data	SWS_SecOC_00212

7 Functional specification

Authentication and integrity protection of sensitive data is necessary to protect correct and safe functionality of the vehicle systems – this ensures that received data comes from the right ECU and has the correct value.

The SecOC module aims for resource-efficient and practicable authentication mechanisms of sensitive data on the level of PDUs. The approach proposed in this specification generally supports the use of symmetric and asymmetric methods for authenticity and integrity protection. Both methods roughly aim at the same goal and show major similarities in the concept, but there are also some differences due to differing technical properties of the underlying primitives. In addition, the commonly used terms for Authenticator are different. In general, the term Message Authentication Code (MAC) is used for symmetric approaches while the term signature or digital signature refers to asymmetric approaches having different properties and constraints.

In order to ease presentation and improve legibility, the following approach is taken: The subsequent section describes the technical approach using symmetric mechanisms in some detail. Here also the common terms for symmetric primitives are used. The adaptations that need to be done in case of an asymmetric approach are separately given in section 7.1.4.

7.1 Specification of the security solution

The SecOC module as described in this document provides functionality necessary to verify the authenticity and freshness of PDU based communication between ECUs within the vehicle architecture. The approach requires both the sending ECU and the receiving ECU to implement a SecOC module. Both SecOC modules are integrated providing the upper and lower layer PduR APIs on the sender and receiver side. The SecOC modules on both sides generally interact with the PduR module.

To provide message freshness, the SecOC module on the sending and receiving side get freshness from an external Freshness Manager for each uniquely identifiable Secured I-PDU, i.e. for each secured communication link.

On the sender side, the SecOC module creates a Secured I-PDU by adding authentication information to the outgoing Authentic I-PDU. The authentication information comprises of an Authenticator (e.g. Message Authentication Code) and optionally a Freshness Value. Regardless if the Freshness Value is or is not included in the Secure I-PDU payload, the Freshness Value is considered during generation of the Authenticator. When using a Freshness Counter instead of a Timestamp, the Freshness Counter should be incremented by the Freshness Manager prior to providing the authentication information to the receiver side.

On the receiver side, the SecOC module checks the freshness and authenticity of the Authentic I-PDU by verifying the authentication information that has been appended by the sending side SecOC module. To verify the authenticity and freshness of an Authentic I-PDU, the Secured I-PDU provided to the receiving side SecOC should be

the same Secured I-PDU provided by the sending side SecOC and the receiving side SecOC should have knowledge of the Freshness Value used by the sending side SecOC during creation of the Authenticator.

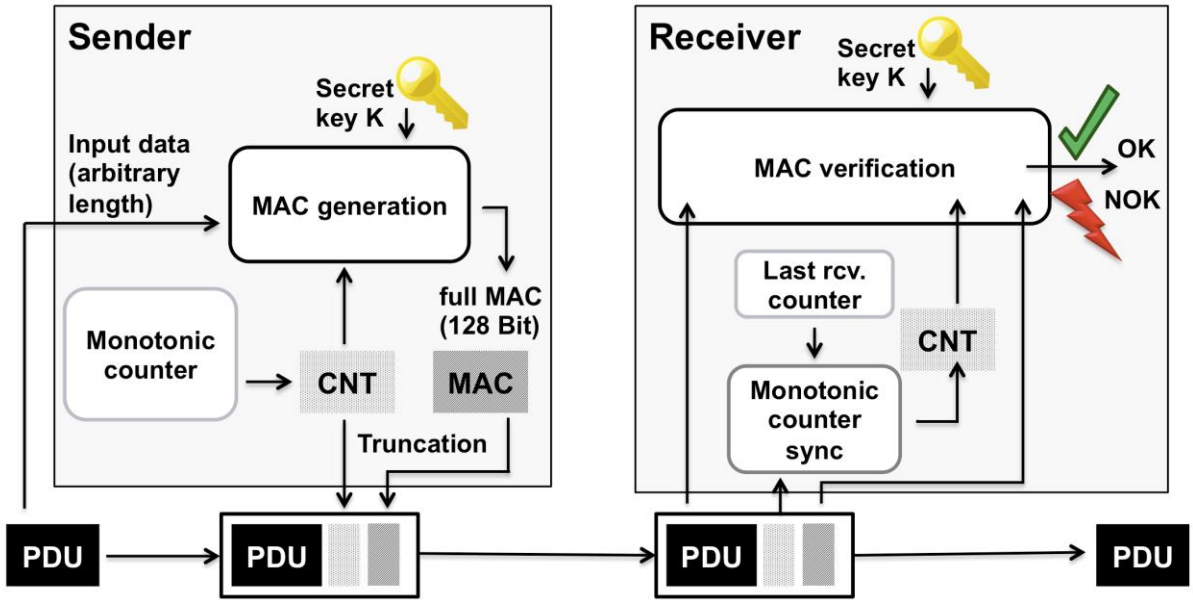

Figure 2: Message Authentication and Freshness Verification

The main purpose of the SecOC module is the realization of the security functionality described throughout this specification.

7.1.1 Basic entities of the security solution

7.1.1.1 Authentic I-PDU and Secured I-PDU

The term Authentic I-PDU refers to an AUTOSAR I-PDU that requires protection against unauthorized manipulation and replay attacks.

The payload of a Secured I-PDU consists of the Authentic I-PDU and an Authenticator (e.g. Message Authentication Code). The payload of a Secured I-PDU may optionally include the Freshness Value used to create the Authenticator (e.g. MAC). The order in which the contents are structured in the Secured I-PDU is compliant with **Figure 3**.

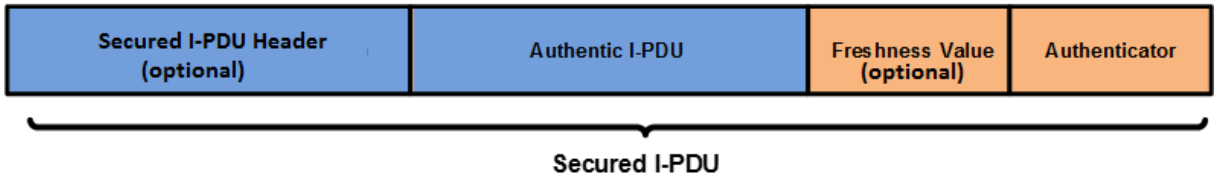

Figure 3: Secured I-PDU contents

The length of the Authentic I-PDU, the Freshness Value and the Authenticator within a Secured I-PDU may vary from one uniquely indefinable Secured I-PDU to another.

The Authenticator (e.g. MAC) refers to a unique authentication data string generated using a Key, Data Identifier of the Secured I-PDU, Authentic Payload, and Freshness Value. The Authenticator provides a high level of confidence that the data in an Authentic I-PDU is generated by a legitimate source and is provided to the receiving ECU at the time in which it is intended for.

Depending on the authentication algorithm(parameter SecOCTxAuthServiceConfigRef or `SecOCRxAuthServiceConfigRef`) used to generate the Authenticator, it may be possible to truncate the resulting Authenticator (e.g. in case of a MAC) generated by the authentication algorithm. Truncation may be desired when the message payload is limited in length and does not have sufficient space to include the full Authenticator.

The Authenticator length contained in a Secured I-PDU (parameter SecOCAuthInfoTruncLength) is specific to a uniquely identifiable Secured I-PDU. This allows provision of flexibility across the system (i.e. two independent unique Secured I-PDUs may have different Authenticator lengths included in the payload of the Secure I-PDU) by providing fine grain configuration of the MAC truncation length for each Secured I-PDU.

If truncation is possible, the Authenticator should only be truncated down to the most significant bits of the resulting Authenticator generated by the authentication algorithm. Figure 5 shows an example of the truncation of the Authenticator and the Freshness Values respecting the parameter SecOCFreshnessValueTruncLength and SecOCAuthInfoTruncLength.

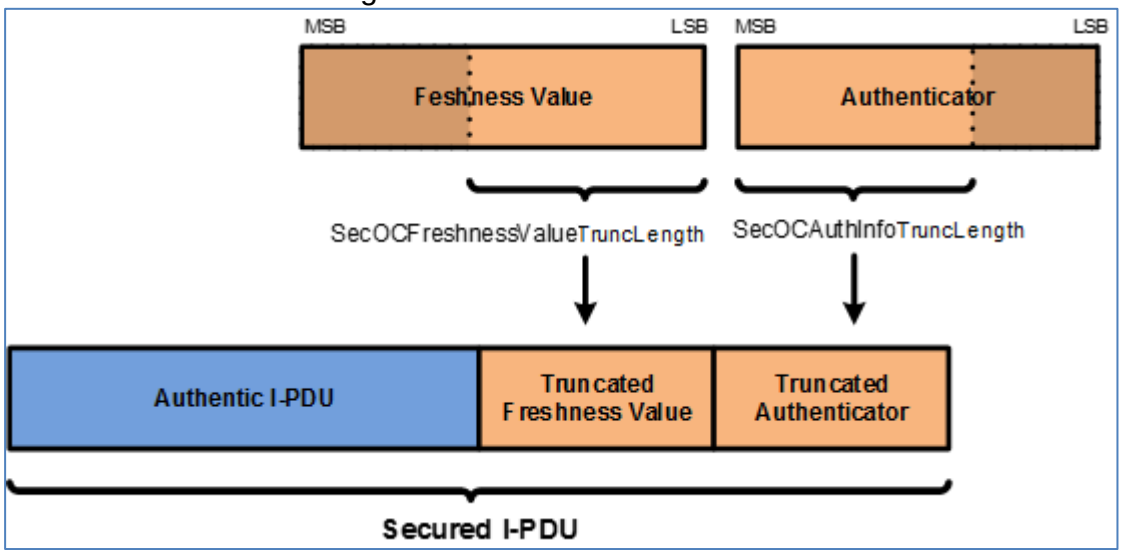

Figure 4: An example of Secured I-PDU contents with truncated Freshness Counter and truncated Authenticator (without Secured I-PDU Header)

Note: For the resource constraint embedded use case with static participants, we propose using Message Authentication Codes (MACs) as a basis for authentication (e.g. a CMAC [16] based on AES [19] with an adequate key length).

Note: In case a MAC is used, it is possible to transmit and compare only parts of the MAC. This is known as MAC truncation. However, this results in a lower security level at least for forgery of single MACs. While we propose to always use a key length of at least 128 bit, a MAC truncation can be beneficial. Of course, the actual length of the MAC for each use case has to be chosen carefully. For

some guidance, we refer to appendix A of [16]. In general, MAC sizes of 64 bit and above are considered to provide sufficient protection against guessing attacks by NIST. Depending on the use case, different MAC sizes can be appropriate, but this requires careful judgment by a security expert.

[SWS_SecOC_00011]⌈
All SecOC data (e.g. Freshness Value, Authenticator, Data Identifier, SecOC message link data,...) that is directly or indirectly transmitted to the other side of a communication link shall be encoded in Big Endian byte order so that each SecOC module interprets the data in the same way.
⌋ (SRS_SecOC_00006)

[SWS_SecOC_00261]⌈
The Secured I-PDU Header shall indicate the length of the Authentic I-PDU in bytes. The length of the Header shall be configurable by the parameter SecOCAuthPduHeaderLength.

Note: the SecOC supports combined usage of authentication data in a separate message (secured PDU collection) and Secured I-PDU Header. Also the SecOC covers dynamic length Authentic I-PDU.
⌋ (SRS_SecOC_00006)

7.1.1.2 Data covered by Authenticator

The data that the Authenticator is calculated on consists of the Data Identifier of the Secured I-PDU (parameter SecOCDataId), Authentic I-PDU data, and the Complete Freshness Value. The Data Identifier of the Secured I-PDU (parameter SecOCDataId), the secured part of the Authentic I-PDU, and the complete Freshness Value are concatenated together respectively to make up the bit array that is passed into the authentication algorithm for Authenticator generation/verification.

DataToAuthenticator = Data Identifier | secured part of the Authentic I-PDU | Complete Freshness Value

Note: “|” denotes concatenation

7.1.1.3 Freshness Values

Each Secured I-PDU is configured with at least one Freshness Value. The Freshness Value refers to a monotonic counter that is used to ensure freshness of the Secured I-PDU. Such a monotonic counter could be realized by means of individual message counters, called Freshness Counter, or by a time stamp value called Freshness Timestamp. Freshness Values are to be derived from a Freshness Manager.

[SWS_SecOC_00094]⌈
If the parameter `SecOCFreshnessValueTruncLength` is configured to a smaller length than the actual freshness value, SecOC shall include only the least significant bits of the freshness value up to `SecOCFreshnessValueTruncLength` within the secured I-PDU.
If the parameter `SecOCFreshnessValueTruncLength` is configured to 0, the freshness value shall not be included in the secured I-PDU.

] (SRS_SecOC_00002, SRS_SecOC_00007)

Note: The larger number of bits of the complete Freshness Value included in the authenticated message payload results in a larger window where the receiver remains synchronized with the transmitters Freshness Value without executing a synchronization strategy.

Note: When including part of the Freshness Value in the authenticated message payload, the Freshness Value is referred to as two parts, the most significant bits and the least significant bits. The part of the counter included in the Secured I-PDU payload is referred to as the least significant bits of the Freshness Value and the remaining part of the counter is referred to as the most significant bits of the Freshness Value.

[SWS_SecOC_00219][

If `SecOCUseAuthDataFreshness` is set to TRUE, SecOC shall use a part of the Authentic I-PDU as freshness. In this case, `SecOCAuthDataFreshnessStartPosition` determines the start position in bits of the freshness inside the Authentic I-PDU and `SecOCAuthDataFreshnessLen` determines its length in bits.

] (SRS_SecOC_00006, SRS_SecOC_00029)

Note: This allows reusing existing freshness values from the payload which are guaranteed to be unique within the validity period of a Freshness Timestamp, e.g. a 4 bit E2E counter. In this case SecOC does not need to generate any additional counter values.

Example:
If `SecOCUseAuthDataFreshness` is set to TRUE, `SecOCAuthDataFreshnessStartPosition` is set to '11' and `SecOCAuthDataFreshnessLen` is set to '4', the following part of the PDU would be extracted:

Byte index of the PDU	0	1	…
Start bit numbering scheme	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	…

For a PDU "AB CD" (hex), the authentic data freshness would be "0110" (bin).

[SWS_SecOC_00220][

The Freshness Manager provides or receives freshness information in interface functions as byte arrays. The freshness is always aligned to the MSB of the first byte in the array. The 8th bit of the freshness is the MSB of the 2nd byte and so on. Unused bits of the freshness array must be set to 0. The associated length information must be given in bits.

] (SRS_SecOC_00029)

Example:
The 10-bit freshness "001101011" (bin) can be located in a 2 byte array and corresponds to the value: "35 80" (hex). The length value is 10.

[SWS_SecOC_00221][

If `SecOCQueryFreshnessValue` = `CFUNC` AND `SecOCProvideTxTruncatedFreshnessValue`= `TRUE` for a PDU configuration, the SecOC calls the interface function `SecOC_GetTxFreshnessTruncData` whenever the `DataToAuthenticator` is constructed for the respective PDU.

] (SRS_SecOC_00029)

[SWS_SecOC_00222]⌈
If `SecOCQueryFreshnessValue` = `CFUNC` AND `SecOCProvideTxTruncatedFreshnessValue`= `FALSE` for a PDU configuration, the SecOC calls the interface function `SecOC_GetTxFreshness` whenever the `DataToAuthenticator` is constructed for the respective PDU.
⌋ (SRS_SecOC_00029)

[SWS_SecOC_00223]⌈
If `SecOCQueryFreshnessValue` = `RTE` AND `SecOCProvideTxTruncatedFreshnessValue`= `TRUE` for a PDU configuration, the SecOC calls the service operation `FreshnessManagement_GetTxFreshnessTruncData` whenever the `DataToAuthenticator` is constructed for the respective PDU.
⌋ (SRS_SecOC_00029)

[SWS_SecOC_00224]⌈
If `SecOCQueryFreshnessValue` = `RTE` AND `SecOCProvideTxTruncatedFreshnessValue`= `FALSE` for a PDU configuration, the SecOC calls the service operation `FreshnessManagement_GetTxFreshness` whenever the `DataToAuthenticator` is constructed for the respective PDU.
⌋ (SRS_SecOC_00029)

[SWS_SecOC_00225]⌈
For every transmission request that is queued to SecOC an authentication build counter shall be maintained.
⌋ (SRS_SecOC_00021, SRS_SecOC_00029)

[SWS_SecOC_00226]⌈
Upon the initial processing of a transmission request of a secured I-PDU SecOC shall set the authentication build counter to 0.
⌋ (SRS_SecOC_00005, SRS_SecOC_00021,SRS_SecOC_00029)

[SWS_SecOC_00227]⌈
If either the query of the freshness function (e.g. `SecOC_GetTxFreshness`()) returns `E_BUSY` or the calculation of the authenticator (e.g. `Csm_MacGenerate`()) returns `E_BUSY`, `QUEUE_FULL` or any other recoverable error, the authentication build counter shall be incremented.
⌋ (SRS_SecOC_00021,SRS_SecOC_00029)

Note: The return value `E_NOT_OK` is not considered as a recoverable error.

[SWS_SecOC_00228]⌈
If building the authentication has failed and the authentication build counter has not yet reached the configuration value `SecOCAuthenticationBuildAttempts`, the freshness attempt and authenticator calculation shall be retried in the next call to the Tx main function.
⌋ (SRS_SecOC_00021, SRS_SecOC_00029)

[SWS_SecOC_00229]⌈
If the authentication build counter has reached the configuration value SecOCAuthenticationBuildAttempts, or the query of the freshness function returns E_NOT_OK or the calculation of the authenticator has returned a non-recoverable error such as returning E_NOT_OK or KEY_FAILURE, the SecOC module shall use SecOCDefaultAuthenticationInformationPattern for all the bytes of Freshness Value and Authenticator to build the Authentication Information if sending SecOCDefaultAuthenticationInformationPattern is enabled by service SecOC_SendDefaultAuthenticationInformation . If sending SecOCDefaultAuthenticationInformationPattern is not enabled, the SecOc module shall remove the Authentic I-PDU from its internal buffer and cancel the transmission request.
⌋ (SRS_SecOC_00021, SRS_SecOC_00029)

Note:
Example:
SecOCFreshnessValueTxLength = 4bits
SecOCAuthInfoTxLength = 20 bits
SecOCDefaultAuthenticatorValue = 0xA5
The resulting default Authentication Information within the secured PDU would be 0x05 (Truncated Freshness Value) | 0xA5 0xA5 0xA0 (Truncated Authenticator). “|” denotes concatenation.

[SWS_SecOC_00230]⌈
If `SecOCQueryFreshnessValue` = `CFUNC` AND `SecOCProvideTxTruncatedFreshnessValue`= `TRUE` for a PDU configuration, SecOC calls a function named `SecOC_GetTxFreshnessTruncData`, to get the current freshness for TX messages.
⌋ (SRS_SecOC_00003, SRS_SecOC_00006, SRS_SecOC_00029)

[SWS_SecOC_00231]⌈
If `SecOCQueryFreshnessValue` = `CFUNC` AND `SecOCProvideTxTruncatedFreshnessValue`= `FALSE` for a PDU configuration, SecOC calls a function named `SecOC_GetTxFreshness`, to get the current freshness for TX messages.
⌋ (SRS_SecOC_00003, SRS_SecOC_00006, SRS_SecOC_00029)

[SWS_SecOC_00232]⌈
If `SecOCQueryFreshnessValue` = `CFUNC` for a PDU configuration, SecOC calls a function with the signature described in SWS_SecOC_91005 to indicate that the Secured I-PDU has been successfully initiated for transmission.
⌋ (SRS_SecOC_00002, SRS_SecOC_00003, SRS_SecOC_00029)

Note: It is not intended, that this function is called after the message has appeared on the bus. It is considered to be more secure calling this function after the successful transmission request to the PduR.

[SWS_SecOC_00233]⌈

If SecOCQueryFreshnessValue = RTE for a PDU configuration, SecOC calls the service operation FreshnessManagement_SPduTxConfirmation to indicate that the Secured I-PDU has been successfully initiated for transmission.
⌋ (SRS_SecOC_00002, SRS_SecOC_00029)

[SWS_SecOC_00234]⌈
For every processed secured I-PDU within SecOC an authentication build counter and an authentication verify attempt counter shall be maintained.
⌋ (SRS_SecOC_00007, SRS_SecOC_00029)

[SWS_SecOC_00235]⌈
Upon the initial processing of a received secured I-PDU, the authentication build counter and the authentication verify attempt counter shall be set to 0.
⌋ (SRS_SecOC_00005, SRS_SecOC_00007, SRS_SecOC_00029)

[SWS_SecOC_00236]⌈
If the query of the freshness function (e.g. SecOC_GetRxFreshness()) returns E_BUSY the authentication build counter shall be incremented and no attempt for verification of authentication shall be executed.
⌋ (SRS_SecOC_00007, SRS_SecOC_00022, SRS_SecOC_00029)

[SWS_SecOC_00237]⌈
If the verification of the authenticator (e.g. Csm_MacVerify()) returns E_BUSY, QUEUE_FULL or any other recoverable error, the authentication build counter shall be incremented.
⌋ (SRS_SecOC_00007, SRS_SecOC_00022, SRS_SecOC_00029)

Note: The return value E_NOT_OK is not considered as a recoverable error.

[SWS_SecOC_00238]⌈
If the authentication build attempts have failed and the authentication build counter has not yet reached the configuration value SecOCAuthenticationBuildAttempts, the freshness attempt and the authenticator verification shall be retried in the next call to the Rx main function.
⌋ (SRS_SecOC_00007, SRS_SecOC_00022, SRS_SecOC_00029)

[SWS_SecOC_00239]⌈
If the verification of the authenticator could be successfully executed but the verification failed (e.g. the MAC verification has failed or the key was invalid), the authentication verify attempt counter shall be incremented and the authentication build counter shall be set to 0.
⌋ (SRS_SecOC_00007, SRS_SecOC_00022, SRS_SecOC_00029)

Note: Resetting the authentication build counter shall prevent to drop the authentication process too early even though authentication verify attempts are still possible.

[SWS_SecOC_00240]⌈

If the authentication build counter has reached the configuration value SecOCAuthenticationBuildAttempts the SecOC module shall remove the Authentic I-PDU from its internal buffer and shall drop the received message. The VerificationResultType shall be set to SECOC_AUTHENTICATIONBUILDFAILURE.

if SecOC_VerifyStatusOverride is used, the verification result and I-PDU are handled according to overrideStatus value.
] (SRS_SecOC_00007, SRS_SecOC_00022, SRS_SecOC_00029)

[SWS_SecOC_00256]⌈
If the query of the freshness function returns E_NOT_OK the SecOC module shall remove the Authentic I-PDU from its internal buffer and shall drop the received message. The VerificationResultType shall be set to SECOC_FRESHNESSFAILURE.
⌋ ()

[SWS_SecOC_00241]⌈
If the authentication verify attempt counter has reached the configuration value SecOCAuthenticationVerifyAttempts or the verification of the authenticator has returned a non-recoverable error such as returning E_NOT_OK or KEY_FAILURE, the SecOC module shall remove the Authentic I-PDU from its internal buffer and shall drop the received message. The VerificationResultType shall be set to SECOC_VERIFICATIONFAILURE.
If SecOC_VerifyStatusOverride is used, the verification result and I-PDU are handled according to overrideStatus value.
⌋ (SRS_SecOC_00007, SRS_SecOC_00022, SRS_SecOC_00029)

Note: The sequence diagram in 9.4 illustrates this behavior.

[SWS_SecOC_00242]⌈
If the verification of the authenticator was successful, the VerificationResultType shall be set to SECOC_VERIFICATIONSUCCESS.
⌋ (SRS_SecOC_00007, SRS_SecOC_00029)

[SWS_SecOC_00243]⌈
The Freshness Management shall use the verification status callout function (SWS_SECOC_00119) to get the result of the verification of a secured I-PDU. This notification can be used as example to synchronize additional freshness attempts or can be used for counter increments.
⌋ (SRS_SecOC_00006, SRS_SecOC_00007, SRS_SecOC_00029)

Note: SecOC allows to overwrite the status (see SWS_SECOC_00142). Therefore, care must be taken if the Freshness Management relies on the status callout while status overwrite function is also used. This can lead to conflicts in the Freshness Management and may lead to incorrect freshness values.

[SWS_SecOC_00244]⌈

If SecOCQueryFreshnessValue = RTE AND SecOCUseAuthDataFreshness = TRUE for a PDU configuration and the secured PDU is received completely, the SecOC calls the Rte service FreshnessManagement_GetRxFreshnessAuthData to query the current freshness. A part of the received PDU data are passed to this service operation as configured by the configuration SecOCAuthDataFreshnessStartPosition and SecOCAuthDataFreshnessLen.
⌋ (SRS_SecOC_00003, SRS_SecOC_00029)

[SWS_SecOC_00245]⌈
If SecOCQueryFreshnessValue = RTE AND SecOCUseAuthDataFreshness = FALSE for a PDU configuration and the secured PDU is received completely, the SecOC calls the Rte service FreshnessManagement_GetRxFreshness to query the current freshness.
⌋ (SRS_SecOC_00003, SRS_SecOC_00029)

[SWS_SecOC_00246]⌈
If SecOCQueryFreshnessValue = CFUNC AND SecOCUseAuthDataFreshness = TRUE for a PDU configuration and the secured PDU is received completely, the SecOC calls the interface function SecOC_GetRxFreshnessAuthData to query the current freshness. A part of the received PDU data are passed to this function as configured by the configuration SecOCAuthDataFreshnessStartPosition and SecOCAuthDataFreshnessLen.
⌋ (SRS_SecOC_00003, SRS_SecOC_00029)

[SWS_SecOC_00247]⌈
If SecOCQueryFreshnessValue = CFUNC AND SecOCUseAuthDataFreshness = FALSE for a PDU configuration and the secured PDU is received completely, the SecOC calls the interface function SecOC_GetRxFreshness to query the current freshness.
⌋ (SRS_SecOC_00003, SRS_SecOC_00029)

[SWS_SecOC_00248]⌈
If the Rx freshness request function returns E_NOT_OK, the verification of an Authentic I-PDU is considered to be failed and the authentication retry counter for this PDU shall be incremented. If the number of authentication attempts has reached SecOCAuthenticationVerifyAttempts, the SecOC module shall remove the Authentic I-PDU from its internal buffer. The failure SECOC_E_RE_FRESHNESS_FAILURE shall be reported to the DET module.
⌋ (SRS_SecOC_00022, SRS_SecOC_00029)

[SWS_SecOC_00249]⌈
If SecOCQueryFreshnessValue = CFUNC AND SecOCUseAuthDataFreshness = TRUE for a PDU configuration, SecOC queries a function named SecOC_GetRxFreshnessAuthData, to get the current freshness for RX messages.
⌋ (SRS_SecOC_00003, SRS_SecOC_00029)

[SWS_SecOC_00250]⌈

If SecOCQueryFreshnessValue = CFUNC AND SecOCUseAuthDataFreshness = FALSE for a PDU configuration, SecOC queries a function named SecOC_GetRxFreshness, to get the current freshness for RX messages.
] (SRS_SecOC_00003, SRS_SecOC_00029)

7.1.2 Authentication of I-PDUs

[SWS_SecOC_00031][
The creation of a Secured I-PDU and thus the authentication of an Authentic I-PDUconsists of the following six steps:

1. Prepare Secured I-PDU
2. Construct Data for Authenticator
3. Generate Authenticator
4. Construct Secured I-PDU
5. Increment Freshness Counter
6. Broadcast Secured I-PDU

] (SRS_SecOC_00006)

[SWS_SecOC_00033][
The SecOC module shall prepare the Secured I-PDU. During preparation,SecOC shall allocate the necessary buffers to hold the intermediate and final results of the authentication process.
] (SRS_SecOC_00006)

[SWS_SecOC_00034][
The SecOC module shall construct the DataToAuthenticator, i.e. the data that is used to calculate the Authenticator. DataToAuthenticator is formed by concatenating the full 16 bit representation of the Data Id (parameter SecOCDataId), the secured part of the Authentic I-PDU and the complete Freshness Value corresponding to SecOCFreshnessValueID in the given order. The Data Id and the Freshness Value shall be encoded in Big Endian byte order for that purpose.](SRS_SecOC_00006)

[SWS_SecOC_00035][
The SecOC module shall generate the Authenticator by passing DataToAuthenticator, length of DataToAuthenticator into the Authentication Algorithm corresponding to SecOCTxAuthServiceConfigRef.
] (SRS_SecOC_00006)

[SWS_SecOC_00036][
The SecOC module shall truncate the resulting Authenticator down to the number of bits specified by SecOCAuthInfoTruncLength.
] (SRS_SecOC_00006)

[SWS_SecOC_00037][

The SecOC module shall construct the Secured I-PDU by adding the Secured I-PDU Header (optional), the Freshness Value (optional) and the Authenticator to the Authentic I-PDU.

The scheme for the Secured I-PDU (includes the order in which the contents are structured in the Secured I-PDU) shall be compliant with below:

```
SecuredPDU = SecuredIPDUHeader (optional) | AuthenticIPDU | FreshnessValue [SecOCFreshnessValueTruncLength] (optional) | Authenticator [SecOCAuthInfoTruncLength]
```

⌋ (SRS_SecOC_00006)

Note: The Freshness Counter and the Authenticator included as part of the Secured I-PDU may be truncated per configuration specific to the identifier of the Secured I-PDU. Also, Freshness Value may be a part of Authentic I-PDU (see [SWS_SecOC_00219]).

7.1.3 Verification of I-PDUs

[SWS_SecOC_00040]⌈
The verification of a Secured I-PDU consists of the following six steps:

- Parse Authentic I-PDU, Freshness Value and Authenticator
- Get Freshness Value from Freshness Manager
- Construct Data to Authentication
- Verify Authentication Information
- Send Confirmation to Freshness Manager
- Pass Authentic I-PDU to upper layer

⌋ (SRS_SecOC_00006)

[SWS_SecOC_00203]⌈
If `SecOCRxSecuredPduCollection` is used then SecOC shall not perform any verification until it has received both the Authentic I-PDU and Cryptographic I-PDU which make up the Secured I-PDU. Only after both have been received SecOC shall attempt to verify the resulting Secure I-PDU. If `SecOC_VerifyStatusOverride` is used, the verification result and I-PDU are handled according to `overrideStatus` value.
⌋
(SRS_SecOC_00026, SRS_SecOC_00028)

Note: This applies to all instances when a Secured I-PDU is received by SecOC from the PduR, which happens in parts as described above when `SecOCRxSecuredPduCollection` is used. There is no further distinction made throughout this document to avoid duplication and clutter.

[SWS_SecOC_00211]⌈
If `SecOCRxSecuredPduCollection` is used then SecOC shall not attempt to verify the Secured I-PDU until it has received and buffered an Authentic I-PDU and Cryptographic I-PDU with matching Message Linker values. If `SecOC_VerifyStatusOverride` is used, the verification result and I-PDU are handled according to `overrideStatus` value.
⌋

(SRS_SecOC_00028)

Note: If `SecOCUseMessageLink` has 0 multiplicity, it means `SecOCMessageLinkLen` is 0 and that Message Linker Values are always matching.

[SWS_SecOC_00042]⌈
Upon reception of a secured I-PDU, SecOC shall parse the Authentic I-PDU, the Freshness Value and the Authenticator from it.
⌋ (SRS_SecOC_00006)

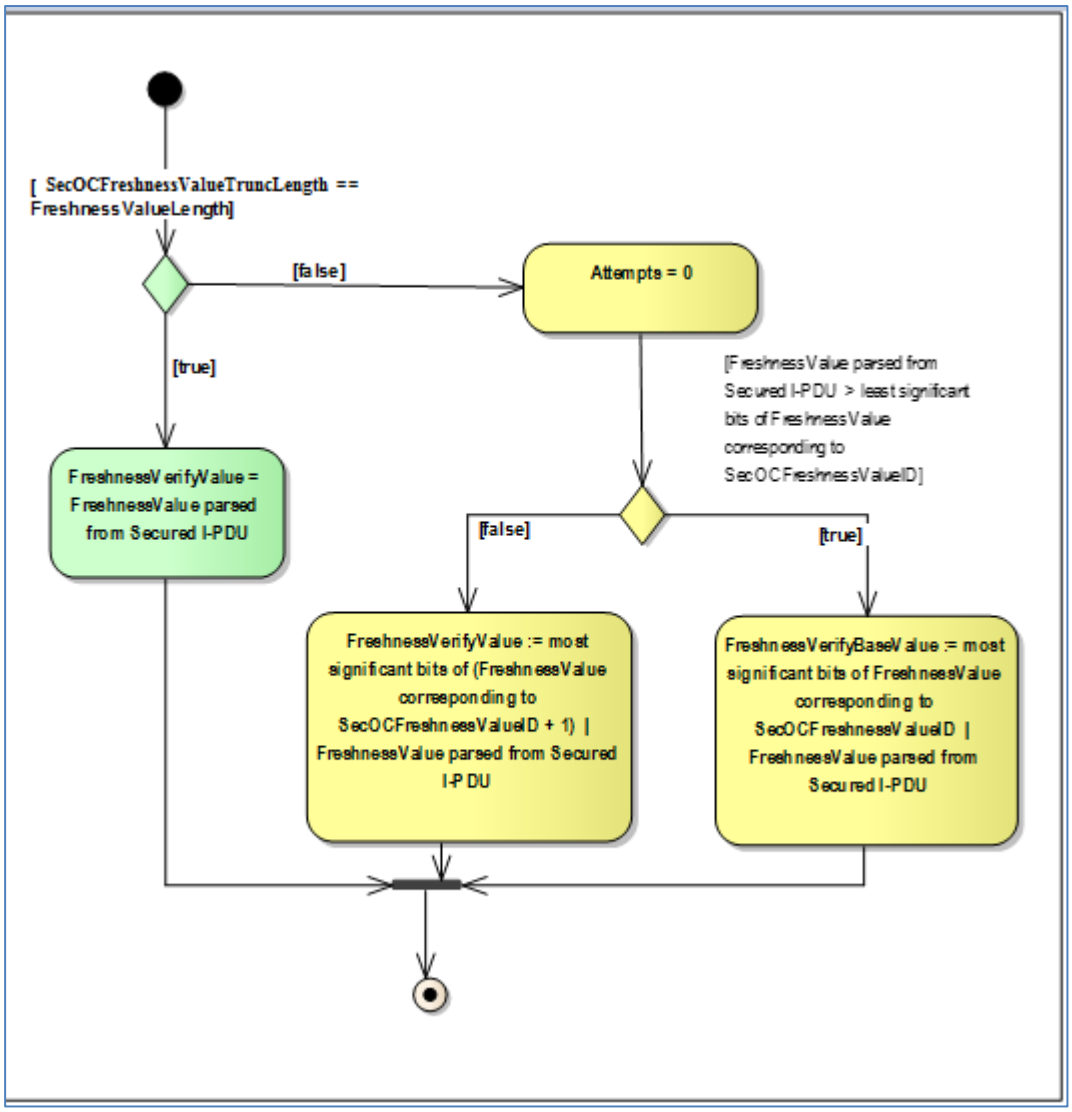

Figure 5: Construction of Freshness Value

[SWS_SecOC_00046]⌈
The SecOC module shall construct the data that is used to calculate the Authenticator (`DataToAuthenticator`) on the receiver side. This data is comprised of `SecOCDataId| AuthenticIPDU | FreshnessVerifyValue`
⌋ (SRS_SecOC_00006)

[SWS_SecOC_00047]⌈

The SecOC module shall verify the Authenticator by passing `DataToAuthenticator`, length of `DataToAuthenticator`, the Authenticator parsed from Secured I-PDU, and `SecOCAuthInfoTruncLength` into the authentication algorithm corresponding to `SecOCRxAuthServiceConfigRef`.
The verification process is repeated as outlined in chapter 9.2.
If `SecOC_VerifyStatusOverride` is used, the verification result and I-PDU are handled according to overrideStatus value.
](SRS_SecOC_00002, SRS_SecOC_00007, SRS_SecOC_00022)

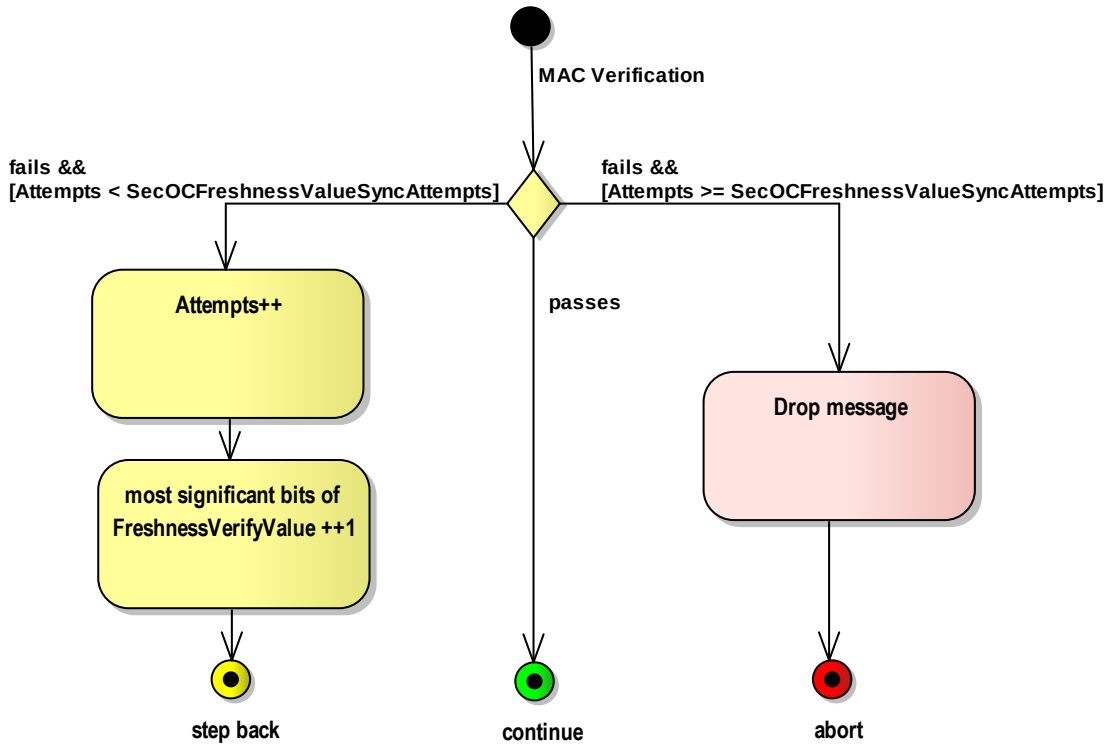

Figure 6: Verification of MAC

[SWS_SecOC_00048][
The SecOC module shall report each individual verification status (the final one as well as all intermediate ones) by serving the call out function `SecOC_VerificationStatusCallout`and the `SecOC_VerificationStatus` interface according to its current configuration (see parameter `SecOCVerificationStatusPropagationMode`).
] (SRS_SecOC_00022)

Note: If the Freshness Manager requires the status of a secured PDU if it was verified successfully or not, e.g. to synchronize time or counter, then this status shall be taken from the VerificationStatus service provided by SecOC.

7.1.3.1 Successful verification of I-PDUs

[SWS_SecOC_00050][
If the verification of a Secured I-PDU was successful or the status override was set accordingly, the SecOC module shall pass the Authentic I-PDU to the upper layer

communication modules using the lower layer interfaces of the PduR.] (SRS_SecOC_00022)

7.1.4 Adaptation in case of asymmetric approach

Although this document consequently uses the terms and concepts from symmetric cryptography, the SecOC module can be configured to use both,symmetric as well as asymmetric cryptographic algorithms.In case of an asymmetric approach using digital signatures instead of the MAC-approach described throughout the whole document, some adaptations have to be made:

1. Instead of a shared secret between sender and (all) receivers, a key pair consisting of public key and secret key is used. The secret (or private) key is used by the sender to generate the signature, the corresponding public keys is used by (all) receiver(s) to verify the signature. The private key must not be feasibly computable from the public key and it shall not be assessable by the receivers.
2. In order to verify a message, the receiver needs access to the complete signature /output of the signature generation algorithm. Therefore, a truncation of the signature as proposed in the MAC case is NOT possible. The parameter `SecOCAuthInfoTruncLength` has to be set to the complete length of the signature.
3. The signature verification uses a different algorithm then the signature generation. So instead of „rebuilding“ the MAC on receiver side and comparing it with the received (truncated) MAC as given above, the receiver / verifier performs the verification algorithm using the `DataToAuthenticator` (including full counter) and the signature as inputs and getting a Boolean value as output, determining whether the verification passed or failed.

7.2 Relationship to PduR

The SecOC module is arranged next to the PDU-Router in the layered architecture of AUTOSAR; see Figure 7.

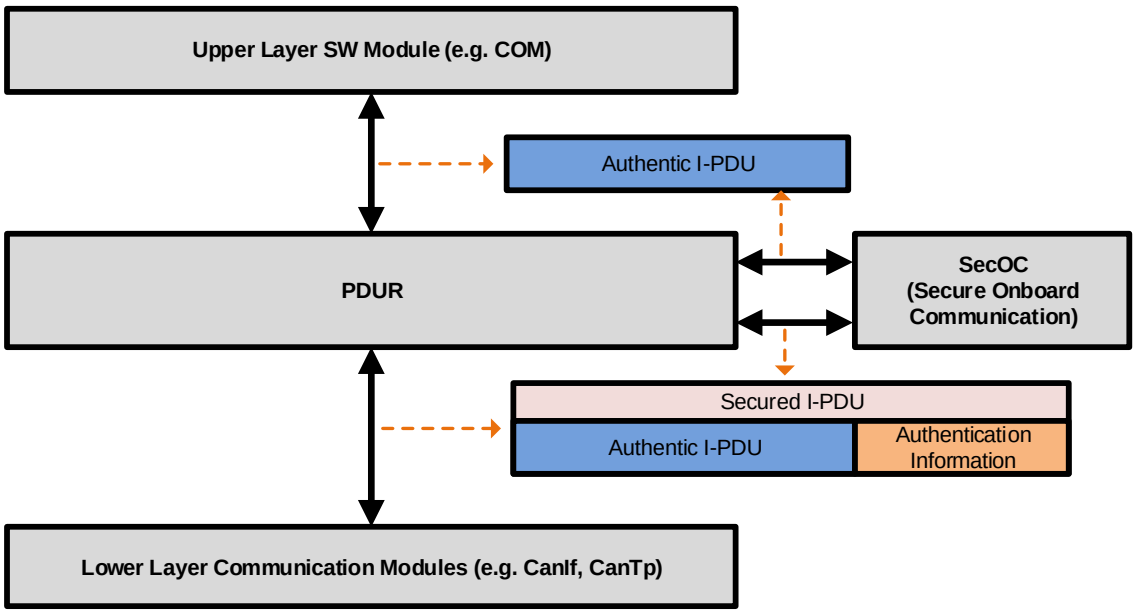

Figure 7:Transformation of an Authentic I-PDU in a Secured I-PDU by SecOC

[SWS_SecOC_00153]⌈
The SecOC module shall be implemented so that no other modules depend on it and that it is possible to build a system without the SecOC module if it is not needed.
⌋ (SRS_BSW_00171)

[SWS_SecOC_00212]⌈
SecOC shall ensure that MetaData received in an authentic PDU will be present unchanged in the corresponding secured PDU, and vice versa.
⌋ (SWS_BSW_00242)

7.3 Initialization

The SecOC module provides an initialization function (`SecOC_Init`) as defined in SWS_SecOC_00106. This function initializes all internal global variables and the buffers to store the SecOC I-PDUs and all intermediate results. The environment of the SecOC shall call `SecOC_Init` before calling any other function of the SecOC module except `SecOC_GetVersionInfo`.The implementer has to ensure that `SecOC_E_UNINIT` is returned in development mode in case an API function is called before the module is initialized.

For the I-PDU data transmission pathway through the SecOC module, a buffer is allocated inside the SecOC module. This buffer needs to be initialized because it might be transmitted before it has been fully populated with data by the upper layer of lower layer communication modules.

[SWS_SecOC_00054]⌈
Within `SecOC_Init`, the module shall initialize all internal global variables and the buffers of the SecOC I-PDUs.

] (SRS_SecOC_00005)

7.4 Authentication of outgoing PDUs

The term authentication describes the creation of a Secured I-PDU by adding Authentication Information to an Authentic I-PDU. This process is described in general terms in Section 7.1.2. This section refines the general description with respect to requirements arising from the integration with the PduR module considering different bus interfaces and transport protocols. In general, the interaction with the PduR module and the authentication of Authentic I-PDUs are organized according to the following scheme:

1. For each transmission request of an Authentic I-PDU, the upper layer communication module shall call the PduR module through `PduR_<Up>Transmit`.
2. The PduR routes this request to the SecOC module and calls `SecOC_[If|Tp]Transmit`.
3. The SecOC module copies the Authentic I-PDU to its own memory and returns.
4. During the next scheduled call of its main function, the SecOC module creates the Secured I-PDU by calculating the Authentication Information and initiates the transmission of the Secured I-PDU by notifying the respective lower layer module via the PduR module.
5. Thereafter, the SecOC module takes the role of an upper layer communication module and thus serves all lower layer requests to provide information on or to copy data of the Secured I-PDU.
6. Finally, the confirmation of the successful or unsuccessful transmission of the Secured I-PDU are provided to the upper layer communication module as confirmation of the successful or unsuccessful transmission of the Authentic I-PDU

Note: For each Authentic I-PDU, the upper layer communication module shall be configured in such a way that it calls the PduR module as it normally does for a direct transmission request. In this case, the upper layer is decoupled from TriggerTransmit and TP behavior by means of the SecOC module.

To initiate the transmission of an Authentic I-PDU, the upper layer module always (and independent of the bus interface that is used for the concrete transmission) calls the PduR module through `PduR_<Up>Transmit`. The PduR routes this request to the SecOC module so that the SecOC module has immediate access to the Authentic I-PDU in the buffer of the upper layer communication module.

[SWS_SecOC_00252]⌈
The SecOC module shall copy the complete Authentic I-PDU to its internal memory before starting transmission of the corresponding Secured I-PDU.
] (SRS_SecOC_00032)

Note: This means there is no dependency between the IF/TP configuration of Up versus Lower PDU interfaces.

[SWS_SecOC_00201]⌈
If `SecOCTxSecuredPduCollection` is used, then SecOC shall transmit the Secured I-PDU as two messages: The original Authentic I-PDU and a separate

Cryptographic I-PDU. The Cryptographic I-PDU shall contain all Authentication Information of the Secured I-PDU, so that the Authentic I-PDU and the Cryptographic I-PDU contain all information necessary to reconstruct the Secured I-PDU.
](SRS_SecOC_00026)

Note: This applies to all instances when a Secured I-PDU is transmitted by SecOC to the PduR. There is no further distinction made throughout this document to avoid duplication and clutter.

[SWS_SecOC_00202][
SecOC shall transmit an Authentic I-PDU and its corresponding Cryptographic I-PDU within the same main function cycle.
](SRS_SecOC_00026)

[SWS_SecOC_00209][
If `SecOCTxSecuredPduCollection` is used then SecOC shall repeat a part of the Authentic I-PDU inside the Cryptographic I-PDU as Message Linker and the Cryptographic I-PDU shall be constructed as
`Cryptographic I-PDU =Authentication Data | Message Linker`
](SRS_SecOC_00028)

Note: "|" denotes concatenation.

[SWS_SecOC_00210][
If `SecOCUseMessageLink` is used then SecOC shall use the value at bit position `SecOCMessageLinkPos` of length `SecOCMessageLinkLen` bits inside the Authentic I-PDU as the Message Linker.
](SRS_SecOC_00028)

[SWS_SecOC_00057][
The SecOC module shall provide sufficient buffer capacities to store the incoming Authentic I-PDU, the outgoing Secured I-PDU and all intermediate data of the authentication process according to the process described in SWS_SecOC_00031.
] (SRS_SecOC_00006)

[SWS_SecOC_00146][
The SecOC module shall provide separate buffers for the Authentic I-PDU and the Secured I-PDU.
] (SRS_SecOC_00006)

[SWS_SecOC_00110][
Any transmission request from the upper layer communication module shall overwrite the buffer that contains the Authentic I-PDU without affecting the buffer of the respective Secured I-PDU.
] (SRS_BSW_00426)

Thus, upper layer updates for Authentic I-PDUs could be processed without affecting ongoing transmission activities of Secured I-PDUs with the lower layer communication module.

[SWS_SecOC_00262][

For a Tx Secured I-PDU with SecOCAuthPduHeaderLength > 0, the SecOC module shall add the Secured I-PDU Header to the Secured I-PDU with the length of the Authentic I-PDU within the Secured I-PDU, to handle dynamic Authentic I-PDU.

Note: Primary purpose of this Header is to indicate the position of Freshness Value and Authenticator in Secured I-PDUs with dynamic length Authentic I-PDU.Also some buses which cannot select arbitrary length of L-PDU (e.g. CAN FD and FlexRay) require this Header, because the position of Freshness Value and Authenticator is not always at the end of the Secured I-PDU, as lower layer modules (e.g. CanIf and FrIf) may add bus-specific padding bytes after processing at SecOC (then the L-PDU containing the Secured I-PDU with padding will be: Secured I-PDU = Secured I-PDU Header | Authentic I-PDU | Freshness Value | Authenticator | Bus-specific padding).
⌋ (SRS_SecOC_00006)

7.4.1 Authentication during direct transmission

For transmission of an Authentic I-PDU using bus interfaces that allow ad-hoc transmission (e.g. CanIf), the PDU Router module triggers the transmit operation of the SecOC module for an Authentic I-PDU.In this case, the SecOC module prepares the creation of aSecured I-PDUon basis of the Authentic I-PDU by allocating internal buffer capacities and by copying the Authentic I-PDU to a local buffer location. Afterwards it returns from `SecOC_[If|Tp]Transmit`.

[SWS_SecOC_00058]⌈
The SecOC module shall allocate internal buffer capacities to store the Authentic I-PDU and the Authentication Information in a consecutive memory location.
⌋ (SRS_SecOC_00006)

The actual creation of the Secured I-PDU is processed during the next subsequent call of the scheduled main function. This includes calculating the Authentication Information according to SWS_SecOC_00031 and adding the Authentication Information (i.e. the Authenticator and the possibly truncated Freshness Value) consecutively to the buffer location directly behind the Authentic I-PDU. Thereafter, SecOC module triggers the transmission of the Secured I-PDU to the destination lower layer module by calling `PduR_SecOCTransmit` at the PduR.

[SWS_SecOC_00060]⌈
For transmission of Authentic I-PDUs using bus interfaces that allow ad-hoc transmission (e.g. CanIf), the SecOC module shall calculate the Authenticator in the scheduled main function according to the overall approach specified in SWS_SecOC_00031.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00061]⌈
For transmission of Authentic I-PDUs using bus interfaces that allow ad-hoc communication (e.g. CanIf), the SecOC module shall create the Secured I-PDU in the scheduled main function.

] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00062]⌈
The SecOC module shall provide the complete Secured I-PDU for further transmission to the destination lower layer module by triggering `PduR_SecOCTransmit`.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00063]⌈
If the PDU Router module notifies the SecOC module that the destination lower layer module has either confirmed the transmission of the Secured I-PDU or reported an error during transmission by calling `SecOC_[If|Tp]TxConfirmation`, the SecOC module shall pass the received result of the respective Authentic I-PDU to the upper layer module by calling `PduR_SecOC[If|Tp]TxConfirmation`.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00064]⌈
For transmission of Authentic I-PDUs using bus interfaces that allow ad-hoc communication (e.g. CanIf), the SecOC module shall free the buffer that contains the Secured I-PDU if `SecOC_TxConfirmation` is called for the Secured I-PDU.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

7.4.2 Authentication during triggered transmission

For transmission of an Authentic I-PDU using bus interfaces that allow triggered transmission (e.g. FrIf), the upper layer is configured in such a way that it calls the PduR module like it normally does for a direct transmission. Thus, the upper layer module immediately provides access to the Authentic I-PDU by providing the required buffer information through `PduR_<Up>Transmit`. The PduR forwards this transmission request to the SecOC module by calling SecOC_TriggerTransmit.

Note: Authentication for triggered transmission is only supported, if the upper layer initiates the transmission by explicitly calling `PduR_<Up>Transmit` in before. Triggered transmission in mode `AlwaysTransmit` shall not be used.

In turn, the SecOC module allocates sufficient buffer capacities to store the Authentic I-PDU, the Secured I-PDU and all intermediate data of the authentication process. The SecOC module copies the Authentic I-PDU into its own buffer and returns (see SWS_SecOC_00057, SWS_SecOC_00058, SWS_SecOC_00059).

The actual creation of the Secured I-PDU is processed during the subsequent call of the scheduled main function. This includes calculating the Authentication Information according to SWS_SecOC_00031 and adding the Authentication Information (i.e. the Authenticator and the possibly truncated Freshness Value) consecutively to the buffer location directly behind the Authentic I-PDU. Thereafter, SecOC module triggers the transmission of the Secured I-PDU to the destination lower layer module by calling `PduR_SecOCTransmit` at the PduR.

[SWS_SecOC_00065]⌈

For transmission of Authentic I-PDUs using bus interfaces that allow triggered transmission (e.g. FrIf), the SecOC module shall calculate the Authenticator in the scheduled main function according to the overall approach specified in SWS_SecOC_00031.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00066][
For transmission of Authentic I-PDUs using bus interfaces that allow triggered transmission (e.g. FrIf), the SecOC module shall create the Secured I-PDU in the scheduled main function.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

In the following, the SecOC module serves as a data provider for the subsequent transmission request from the lower layer module. Thus, the SecOC module holds the complete Secured I-PDU and acts as the upper layer module. The upper layer module does not expect any further call back that request the copying of the Authentic I-PDU to the lower layer module.

[SWS_SecOC_00067][
For transmission of Authentic I-PDUs using bus interfaces that allow triggered transmission (e.g. FrIf), the SecOC module shall indicate the transmission request for the complete Secured I-PDU by triggering `PduR_SecOCTransmit` at the PduR. The PduR is responsible to further process the request and to notify the respective lower layer module.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

The destination lower layer module calls `PduR_<Lo>TriggerTransmit` when it is ready to transmit the Secured I-PDU. PduR forwards this request to the SecOC module and the SecOC module copies the complete Secured I-PDU to the lower layer. Afterwards it returns.

Note: The SecOc module must not forward the trigger transmit call to the upper layer but takes itself the role of the upper layer and copies the complete Secured I-PDU to the lower layer.

[SWS_SecOC_00068][
When `SecOC_TriggerTransmit` is called by the PduR module, the SecOC module shall copy the Secured I-PDU to the lower layer destination module.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00150][
When `SecOC_TriggerTransmit` is called by the PduR module and the SecOC module is not able to provide a Secured I-PDU to the lower layer (no Secured I-PDU available), the SecOC module shall return the call with `E_NOT_OK`.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

Finally, when the lower layer confirms the processing of the Secured I-PDU via `PduR_<Lo>TxConfirmation` (the result can be positive, if the PDU was successfully sent or negative if a transmission was not possible), the confirmation is forwarded to the SecOC module by calling `SecOC_TxConfirmation`. In turn, the SecOC module passes the result of the transmission process of the Authentic I-PDU

at the PduR module so that the PduR module could forward the result via `<Up>_TxConfirmation` to the upper layer module which was the source of the original I-PDU (see SWS_SecOC_00063).

During triggered transmission, the update rates of the upper layer modules and the lower layer modules might be different. Thus, the lower layer module might request a new transmission of a Secured I-PDU while the upper layer has not updated the Authentic I-PDU. In this case, the SecOC module supports the repeated transmission of the Authentic I-PDU by means of an updated Secure I-PDU. Thus, it has to preserve the Authentic I-PDU until the Secured I-PDU has been sent and its transmission has been confirmed by a means of `SecOC_TxConfirmation`. In this case, the SecOC module treats the existing Authentic I-PDU as new and re-authenticates it during the subsequent call to the `SecOC_MainFunctionTx`.

[SWS_SecOC_00069]⌈
For transmission of Authentic I-PDUs using bus interfaces that allow triggered transmission (e.g. FrIf) and the transmission of the Secured I-PDU was confirmed by `SecOC_TxConfirmation` (successfully sent), the SecOC module shall free the buffer that contain Authentication Information and preserve the buffer that contain the Authentic I-PDU. The Authentic I-PDU shall be treated as if it has been set by the upper layer and thus shall undergo a new authentication procedure with the subsequent call of the `SecOC_MainFunctionTx`.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

7.4.3 Authentication during transport protocol transmission

For transmission of an Authentic I-PDU using transport protocol transmission (e.g. CanTP, FrTp), the PDU Router module triggers the transmit operation of the SecOC module for an Authentic I-PDU.In this case, the SecOC module prepares the creation of a Secured I-PDU on basis of the Authentic I-PDU by allocation internal buffer capacities and by copying the Authentic I-PDU to a local buffer location. Afterwards it returns from `SecOC_[If|Tp]Transmit`.

The actual creation of the Secured I-PDU is processed during the next following call of the scheduled main function. This includes calculating the Authentication Information according to SWS_SecOC_00031 and adding the Authentication Information(i.e. the Authenticator and the possibly truncated Freshness Value) consecutively to the buffer location directly behind the Authentic I-PDU.

[SWS_SecOC_00253]⌈
In case SecOCPduType is configured to `SECOC_TPPDU`, then function `SecOC_TpTransmit` shall trigger the transmit operation for an Authentic I-PDU.
⌋ ()

[SWS_SecOC_00254]⌈
After a transmit operation for SecOCPduType of `SECOC_TPPDU` was triggered, the SecOC shall instruct the upper layer to copy the next part of the I-PDU to a local SecOC buffer by calling `PduR_SecOCTpCopyTxData`.
⌋ ()

Note: The call to `PduR_SecOCTpCopyTxData` may happen in the context of `SecOC_TpTransmit`.

[SWS_SecOC_00070]⌈
For transmission of Authentic I-PDUs using transport protocol, the SecOC module shall calculate the Authenticator in the scheduled main function according to the overall approach specified in SWS_SecOC_00031. In case `SecOCPduType` is configured to `SECOC_TPPDU` the freshness value shall be retrieved as late as possible i.e. just in time when this part of the message will be transmitted next to the bus.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)
Note: The late freshness value retrieval is necessary to have an up-to-date value for the case that the TP transmission took a while

[SWS_SecOC_00071]⌈
For transmission of Authentic I-PDUs using transport protocol, the SecOC module shall create the Secured I-PDU in the scheduled main function.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

Thereafter, SecOC module triggers the transmission of the Secured I-PDU to the destination lower layer module by calling `PduR_SecOCTpStartOfReception` at the PduR. Thus, it notifies the lower level module about its transmission request for the Secured I-PDU.

[SWS_SecOC_00072]⌈
For transmission of Authentic I-PDUs using transport protocol, the SecOC module shall indicate the transmission request for the complete Secured I-PDU by triggering `PduR_SecOCTransmit` at the PduR. The PduR is responsible to further process the request and to notify the respective lower layer module.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

In the following, the SecOC module serves as a data provider for the subsequent transmission request from the lower layer module. Thus, the SecOC module holds the complete Secured I-PDU and acts as the upper layer module. The upper layer module does not expect any further call back that request the copying of the Authentic I-PDU to the lower layer module.

When the PduR iteratively polls the SecOC module by means of `SecOC_CopyTxData` to effectively transmit the Secured I-PDU to a lower layer module, the SecOC module copies the NPDUs for the Secured I-PDU to the lower layer transport protocol module.

[SWS_SecOC_00073]⌈
For transmission of Authentic I-PDUs using transport protocol, the SecOC module shall copy the NPDUs addressed by `SecOC_CopyTxData` into the buffer of the transport protocol module. After each copy process, it returns from `SecOC_CopyTxData`.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

Finally, when the lower layer confirms the processing of the Secured I-PDU via PduR_<Lo>TxConfirmation (the result can be positive, if the PDU was successfully sent or negative if a transmission was not possible), the result is forwarded to the SecOC module and the SecOC module in turn confirms the processing of the Authentic I-PDU, so that the PduR module could forward the result via <Up>_TxConfirmation to the upper layer.

[SWS_SecOC_00074]⌈
For transmission of Authentic I-PDUs using transport protocol and when the lower Layer either confirms the transmission of the Secured I-PDU or signals an error during transmission by calling SecOC_TpTxConfirmation, the SecOC module shall in turn pass the received result of the Authentic I-PDU either by PduR_SecOCIfTxConfirmation in case SecOCPduType is configured to SECOC_IFPDU or by PduR_SecOCTpTxConfirmation in case SecOCPduType is configured to SECOC_TPPDU.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00075]⌈
For transmission of Authentic I-PDUs using transport protocol, the SecOC module shall free the buffer that contains the Secured I-PDU only, if SecOC_TpTxConfirmation is called for the Secured I-PDU.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

7.4.4 Error handling and cancelation of transmission

[SWS_SecOC_00076]⌈
If the upper layer module requests a cancelation of an ongoing transmission of the Authentic I-PDU by calling SecOC_[If|Tp]CancelTransmit, the SecOC module shall immediately inform the lower layer transport protocol module to cancel the ongoing transmission of the Secured I-PDU, stop all internal actions related to the Authentic I-PDU, and free all related buffers.
⌋ (SRS_SecOC_00021)

[SWS_SecOC_00077]⌈
If the lower layer transport protocol module reports an error during transmission of a Secured I-PDU using the return value E_NOT_OK, the SecOC module shall not perform any error handling other than skipping the confirmation of the transmission request for the corresponding Authentic I-PDU to the upper layer module.
⌋ (SRS_BSW_00385)

[SWS_SecOC_00151]⌈
If the CSM module reports a recoverable error (example: E_BUSY, QUEUE_FULL) during authentication of an Authentic I-PDU , the SecOC module shall not provide a Secured I-PDU to the lower layer. It shall keep that Authentic I-PDU (if not overwritten by an incoming Authentic I-PDU of the same type) to start the authentication with the next call of the scheduled main function until the number of additional authentication attempts for that Authentic I-PDU has reached its limits.
⌋ (SRS_SecOC_00021, SRS_BSW_00385)

[SWS_SecOC_00155]⌈
If the number of attempts for an Authentic I-PDU has reached the limit SecOCAuthenticationBuildAttempts that defines the maximum number of freshness values provided by the freshness manager, the SecOC module shall report SECOC_E_CRYPTO_FAILURE to the DET module.
⌋ (SRS_BSW_00385)

[SWS_SecOC_00108]⌈
If the SecOC module is not able to serve any upper layer or lower layer request during transmission of an Authentic I-PDU due to an arbitrary internal error, it shall return this request with `E_NOT_OK`.
⌋ (SRS_BSW_00385)

[**SWS_SecOC_00217**]⌈
If the upper layer module requests a cancelation of an ongoing reception of the Authentic I-PDU by calling `SecOC_TpCancelReceive`, the SecOC module shall immediately inform the lower layer transport protocol module to cancel the ongoing reception of the Secured I-PDU, stop all internal actions related to the Authentic I-PDU, and free all related buffers.
⌋ (SRS_SecOC_00021)

[**SWS_SecOC_00218**]⌈
If the upper layer module requests a change of parameters of the Authentic I-PDU by calling `SecOC_ChangeParameter`, the SecOC module shall immediately inform the lower layer transport protocol module.
⌋ (SRS_SecOC_00021)

[SWS_SecOC_00260]⌈
If the upper layer transport protocol module reports `BUFREQ_E_BUSY` in a call to `PduR_SecOCTpCopyTxData` then SecOC shall retry the call in the next subsequent call of its scheduled main function.
⌋ ()

[SWS_SecOC_00266] ⌈
If the upper layer transport protocol module reports `BUFREQ_E_NOT_OK` in a call to `PduR_SecOCTpCopyTxData` then SecOC shall immediately abort the transmission via calling `PduR_SecOCTpTxConfirmation` with `E_NOT_OK` result, shall stop all internal actions related to the Authentic I-PDU, and shall free all related buffers.
⌋ ()

7.5 Verification of incoming PDUs

The term verification describes the process of comparing the Authentication Information contained in a Secured I-PDU with the Authentication Information calculated on basis of the local Data Identifier, the local Freshness Value and the Authentic I-PDU contained in the Secured I-PDU.

The process of verifying incoming Secured I-PDUs is described in general terms in Section 7.1.3. This section refines the general description with respect to requirements arising from the integration with the PduR module considering different bus interfaces and transport protocols. The overall interaction with the PduR module and the verification of Secured I-PDUs is organized as described in the following scheme:

1. For each indication of an incoming Secured I-PDU from a lower layer bus interface or transport protocol module, the SecOC module takes the role of an upper layer communication module and thus serves all lower layer requests that are necessary to receive the complete Secured I-PDU.
2. The SecOC module copies the Secured I-PDU into its own memory.
3. Thereafter, when the complete Secured I-PDU is available and during the next scheduled call of its main function, the SecOC module verifies the contents of the Secured I-PDU according to SWS_SecOC_00040.
4. If the verification fails and the parameter `SecOCIgnoreVerificationResult` is configured to `FALSE`, the SecOC module drops the Secured I-PDU.
5. If the verification succeeds or the verification fails and the parameter `SecOCIgnoreVerificationResult` is configured to TRUE, the SecOC module takes the role of a lower layer communication module and calls `PduR_SecOC[If|Tp]RxIndication` for the Authentic I-PDU.
6. The SecOC reports the verification results according to SWS_SecOC_00048.

Thus, SecOC decouples the interaction between upper layer modules and lower layer modules. The SecOC module manages the interaction with lower layer module until it has copied the complete Secured I-PDU into its own buffer. It does so without affecting the upper layer module. Thereafter, it verifies the contents of the Secured I-PDU and, dependent on the verification results, initiates the transmission of the Authentic I-PDU to the upper layer communication module.

[**SWS_SecOC_00214**][
In case the `SecOCReceptionOverflowStrategy` is set to `REPLACE`, the SecOC module shall free all buffer related to a Secured I-PDU if the reception of a Secured I-PDU with the same Pdu Identifier has been initiated.
] (SRS_SecOC_00021, SRS_SecOC_00022)

[**SWS_SecOC_00215**][
In case the `SecOCReceptionOverflowStrategy` is set to `REJECT` and SecOC is currently busy with the same Secured I-PDU, the SecOC module shall ignore any subsequent call of `SecOC_RxIndication` and return `BUFREQ_E_NOT_OK` for any subsequent call of `SecOC_StartOfReception`.
] (SRS_SecOC_00021, SRS_SecOC_00022)

[SWS_SecOC_00204][
SecOC shall provide separate buffers for the incoming Secured I-PDU, Cryptographic I-PDU and the resulting Authentic I-PDU.
](SRS_SecOC_00026)

Note: Thus, lower layer updates of Secured I-PDUs could be processed without affecting

ongoing deliveries of an Authentic I-PDU to the upper layer communication modules.

[**SWS_SecOC_00216**]⌈
In case the `SecOCReceptionOverflowStrategy` is set to `QUEUE` and SecOC is currently busy with the same Secured I-PDU, the SecOC module shall additionally receive the Secured I-PDU and queue them for a subsequent processing after the currently processed Secured I-PDU is finalized. In case the limit which is given by `SecOCReceptionQueueSize` is reach any further reception shall be rejected.
⌋ (SRS_SecOC_00021, SRS_SecOC_00022)

[SWS_SecOC_00205]⌈
For each Secured I-PDU having `SecOCRxSecuredPduCollection` present in the corresponding `SecOCRxSecuredPduLayer` SecOC shall buffer only the last Authentic I-PDU and Cryptographic I-PDU it has received. If a buffer has already been filled with a previous I-PDU, the previous I-PDU is overwritten.
⌋(SRS_SecOC_00026)

Note: An Authentic I-PDU and its corresponding Cryptographic I-PDU must be received in direct succession but their order does not matter. This can be realized for example via priority handling dependent on the underlying bus system.

[SWS_SecOC_00206]⌈
SecOC shall construct and the Secured I-PDU immediately after it has received both the respective Authentic I-PDU and Cryptographic I-PDU. If `SecOC_VerifyStatusOverride` is used, the verification result and I-PDU are handled according to `overrideStatus` value.
⌋(SRS_SecOC_00026)

[SWS_SecOC_00207]⌈
If the subsequent verification of the resulting Secured I-PDU is successful, then SecOC shall clear the buffers of both the Authentic and Cryptographic I-PDU.
⌋(SRS_SecOC_00026)

[SWS_SecOC_00257]⌈
For a Secured Rx I-PDU with `SecOCAuthPduHeaderLength` = 0 or not configured and DynamicLength of the referred global Pdu (see ECUC_EcuC_00078) is set to FALSE, the SecOC module shall extract the Authentic I-PDU by using the configured length of the corresponding global PDU.
⌋ ()

[SWS_SecOC_00258]⌈
For a Secured Rx I-PDU with `SecOCAuthPduHeaderLength` = 0 or not configured and DynamicLength of the referred global Pdu (see ECUC_EcuC_00078) is set to TRUE, the SecOC module shall extract the Authentic I-PDU by using the length provided by the lower layer.
⌋ ()

[SWS_SecOC_00259]⌈

For a Secured Rx I-PDU with `SecOCAuthPduHeaderLength` > 0, the SecOC module shall extract the Authentic I-PDU using the length provided at runtime within the Secured I-PDU Header.
] ()

7.5.1 Verification during bus interface reception

When a Secured I-PDU is received by means of a lower layer bus interface(e.g. CanIf, FrIf), the PduR module calls `SecOC_RxIndication` to inform the SecOC module for each incoming Secured I-PDU. During the processing of `SecOC_RxIndication`, the SecOC module copies the Authentic I-PDU to its own buffer.

[SWS_SecOC_00268][
During reception of a static length (Secured / Authentic / Cryptographic) I-PDU, i.e. EcuC Parameter DynamicLength (ECUC_EcuC_00078) is set to FALSE, by means of a lower layer bus interface and when `SecOC_RxIndication` has been called, the SecOC module shall silently discard this I-PDU in case of the received length is smaller than the configured length.
] ()

Note: Static PDUs will normally be sent with configured length, therefore a mismatch between received length and configured length is seen as an error scenario. Also as static PDUs do not contain header length Information it could lead to errors in case of a shorter length in combination with padding bytes.

[SWS_SecOC_00078][
During reception of an (Secured / Authentic / Cryptographic) I-PDU by means of a lower layer bus interface and when `SecOC_RxIndication` has been called, the SecOC module shall copy the I-PDU into the according buffer according to the minimum of received length and configured length of this I-PDU. The copied length shall then be used for all further reception processings.
] (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

Note: Copying only minimum of configured and passed length ensures that buffer cannot be overwritten and that non-expected data (which was maybe added due to padding) is discarded. For reception from TP this restriction is not needed as TP ensures a valid length value passed. For dynamic length PDUs with a shorter length than configured only the length provided will be copied. Also for dynamic length PDUs TPS_SYST_02189 ensures that a reliable length information is available.

Thereafter, the actual verification of anincoming Secured I-PDU is initiated during the next call of the scheduled main function. The SecOC module extracts the Authentic I-PDU, the Authentication Information from the Secured I-PDU. The SecOC module verifies the authenticity and freshness of the Authentic I-PDU according to SecOC_SWS_0040. If the verification is successful, the SecOC indicates the reception of the Authentic I-PDU by calling `PduR_SecOC[If|Tp]RxIndication` for the Authentic I-PDU. If the verification fails, the SecOC drops the PDU and does not call `PduR_SecOC[If|Tp]RxIndication`.

[SWS_SecOC_00079]⌈
During reception of a Secured I-PDU that is received by means of a lower layer bus interface, the SecOC module shall verify the Authenticator according to the overall approach specified in SWS_SecOC_00040. The verification shall be processed in the scheduled main function.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00080]⌈
During reception of a Secured I-PDU that is received by means of a lower layer bus interface and if the verification eventually succeeds, the SecOC module shall call `PduR_SecOC[If|Tp]RxIndication` referencing the Authentic I-PDU that is contained in the Secured I-PDU.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00081]⌈
During reception of a Secured I-PDU that is received by means of a lower layer bus interface and if the verification fails and the `SecOCIgnoreVerificationResult` is configured to TRUE, the SecOC module shall call `PduR_SecOC[If|Tp]RxIndication` referencing the Authentic I-PDU that is contained in the Secured I-PDU.
⌋(SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

Note: If the verification eventually fails, the SecOC module does not call `PduR_SecOC[If|Tp]RxIndication` for the Authentic I-PDU that is contained in the Secured I-PDU.

7.5.2 Verification during transport protocol reception

When a Secured I-PDU is received by means of a lower layer transport protocol interface (e.g. CanTp, FrTp), the PduR module calls `SecOC_StartOfReception` to notify the SecOC module that the reception process of the respective Secured I-PDU will start.

[SWS_SecOC_00082]⌈
During reception of a Secured I-PDU that is received by means of a lower layer transport protocol interface and when `SecOC_StartOfReception` is called, the SecOC
module shall provide buffer capacities to store the complete Secured I-PDU. Further it shall forward the `SecOC_StartOfReception` call by calling `PduR_SecOCTpStartOfReception` in case `SecOCPduType` is configured to `SECOC_TPPDU`.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

Note: In case the upper layer does not accept the reception, SecOC should not accept the reception as well.

When the lower layer iteratively indicates the reception of the individual NPDUs that constitute the Secured I-PDU (i.e. when `SecOC_CopyRxData` is called), the SecOC module copies the NPDUs to its own buffer.

[SWS_SecOC_00083]⌈
During reception of a Secured I-PDU that is received by means of a lower layer transport protocol interface and when `SecOC_CopyRxData` is called, the SecOC module shall copy the NPDUs addressed by `SecOC_CopyRxData` into its own buffers. Finally, it returns from `SecOC_CopyRxData`.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

Finally, when the lower layer confirms the complete reception of the Secured I-PDU via `SecOC_TpRxIndication` and thus the complete Secured I-PDU is available in the buffer of the SecOC module for further processing, the SecOC module starts the verification of the Authentication Information according to Section 7.1.3 during its next scheduled call of its main function.

[SWS_SecOC_00084]⌈
During reception of a Secured I-PDU that is received by means of a lower layer transport protocol interface and when `SecOC_TpRxIndication` is called, the SecOC module shall returns `SecOC_TpRxIndication` without any further processing.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00085]⌈
During reception of a Secured I-PDU that is received by means of a lower layer transport protocol interface and when `SecOC_TpRxIndication` has been called, the SecOC module shall verify the contents of the Secured I-PDU according to the process described in Section 7.1.3.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00086]⌈
During reception of a Secured I-PDU that is received by means of a lower layer transport protocol interface and when the verification eventually succeeds, the SecOC module shall call `PduR_SecOCIfRxIndication` with references to the Authentic I-PDU contained in the Secured I-PDU in case `SecOCPduType` is configured to `SECOC_IFPDU`.
In case `SecOCPduType` is configured to `SECOC_TPPDU` SecOC shall forward in advance all data to the upper layer by first calling `PduR_SecOCTpCopyRxData` and afterwards `PduR_SecOCTpRxIndication` with references to the Authentic I-PDU contained in the Secured I-PDU.
⌋ (SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[SWS_SecOC_00088]⌈
During reception of a Secured I-PDU that is received by means of a lower layer transport protocol interface and when the verification fails and the `SecOCIgnoreVerificationResult` is configured to TRUE, the SecOC module shall call `PduR_SecOCIfRxIndication` with references to the Authentic I-PDU contained in the Secured I-PDU in case `SecOCPduType` is configured to `SECOC_IFPDU`.

In case SecOCPduType is configured to SECOC_TPPDU SecOC shall forward in advance all data to the upper layer by first calling PduR_SecOCTpCopyRxData and afterwards PduR_SecOCTpRxIndication with references to the Authentic I-PDU contained in the Secured I-PDU.
](SRS_SecOC_00010, SRS_SecOC_00012, SRS_SecOC_00013)

[**SWS_SecOC_00213**][
In case the SecOC frees buffers related to a Secured I-PDU (see SWS_SecOC_00087) and SecOCPduType is configured to SECOC_TPPDU the SecOC shall cancel the reception in the upper layer (negative PduR_SecOCTpRxIndication).
] (SRS_BSW_00385)

[SWS_SecOC_00087][
The SecOC module shall free all buffer related to a Secured I-PDU either if

1. it has passed the respective authenticated I-PDU to the PduR via PduR_SecOCIfRxIndication or PduR_SecOCTpRxIndication,
2. the verification of a Secured I-PDU eventually failed,
3. the transmission of a Secured I-PDU has been canceled by the upper or lower layer.

] (SRS_SecOC_00021, SRS_SecOC_00022)

[SWS_SecOC_00255][
The SecOC module shall receive the complete Secured I-PDU in its internal memory before starting any copying of the corresponding Authentic I-PDU.
] (SRS_SecOC_00032)

7.5.3 Skipping Authentication for Secured I-PDUs at SecOC

[SWS_SecOC_00265][
For a Rx Secured I-PDU with SecOCSecuredRxPduVerification=false, the SecOC module shall extract the Authentic I-PDU without Authentication.
] (SRS_BSW_00385)

7.5.4 Error handling and discarding of reception

[SWS_SecOC_00089][
If the lower layer transport protocol module reports an error by returning something else than E_OK during reception of a Secured I-PDU using SecOC_TpRxIndication, the SecOC module shall drop the Secured I-PDU and free all corresponding buffers.
] (SRS_BSW_00385)

[SWS_SecOC_00121][

If the CSM module reports an error during verification (verification attempt returns E_NOT_OK) of a Secured I-PDU, the SecOC module shall not provide the Authentic I-PDU. It shall keep the Secured I-PDU (if not overwritten by an incoming Secured I-PDU of the same type) and start the verification with the next call of the scheduled main function.
] (SRS_SecOC_00022, SRS_BSW_00385)

[SWS_SecOC_00208]⌈
If SecOC has received both an Authentic I-PDU and a Cryptographic PDU and the verification of the resulting Secured I-PDU fails, both the Authentic and Cryptographic I-PDU shall remain buffered and verification shall be reattempted each time new data for any of them is received.
](SRS_SecOC_00026)

Note: This and the above requirement ensure that even if either an Authentic I-PDU or a Cryptographic I-PDU is lost in transit, SecOC will still function as expected as soon as an Authentic I-PDU and its corresponding Cryptographic I-PDU are received in direct succession.

[SWS_SecOC_00109]⌈
If the SecOC module is not able to serve any upper layer or lower layer request during reception of A Secured I-PDU due to an arbitrary internal error, it shall return this request with E_NOT_OK.
] (SRS_BSW_00385)

[SWS_SecOC_00263]⌈
For a Rx Secured I-PDU with SecOCAuthPduHeaderLength > 0 and the length of Authentic I-PDU in the Header is longer than configured length (in case of dynamic length IPdus (containing a dynamical length signal), this value indicates the maximum data length) of the Authentic I-PDU, the SecOC module shall discard the I-PDU. In such case with SecOC_StartOfReception, BUFREQ_E_NOT_OK shall be returned (see [SWS_COMTYPE_00012]).

Note: SecOC_RxIndication has no return value.
] (SRS_BSW_00385)

[SWS_SecOC_00264]⌈
For a Rx Secured I-PDU with SecOCAuthPduHeaderLength > 0, the SecOC module shall process Secured I-PDU Header, Authentic I-PDU (with the length specified by the Header), Freshness Value and Authenticator of the Rx Secured I-PDU. The rest of bytes in the Secured I-PDU shall be discarded.
] (SRS_BSW_00385)

[SWS_SecOC_00267] ⌈
If the upper layer transport protocol module reports BUFREQ_E_NOT_OK in a call to PduR_SecOCTpCopyRxData then SecOC shall immediately abort the reception via calling PduR_SecOCTpRxIndication with E_NOT_OK result, shall stop all internal actions related to the Secured I-PDU, and shall free all related buffers.
] ()

7.6 Gateway functionality

The SecOC module supports authentication and verification for I-PDUs that are routed from one source bus to one or more destination busses. This allows for the realization of re-authentication gateways that can be used to realize networks with different security zones or properties. The actions necessary to support the required gateway functionality can be simply derived from the authentication and verification scenarios in Sections 7.4 and 7.5. Each authentication or verification process for a given I-PDU need to be configured separately. This functionality includes:

- authentication of outgoing I-PDUs,
- verification of incoming I-PDUs,
- re-authentication gateways, i.e. the verification of incoming I-PDUs in combination of their immediate re-authentication, when the I-PDU is routed to another lower layer module.

Note: “Gatewaying-on-the-fly” is not supported by SecOC

7.7 Multicore Distribution

According to current AUTOSAR architecture it is assumed, the CSM module is only present in one partition. In order to avoid a dependency between the Com-Stack and the Crypto-Stack the PDUs connected to SecOC module should be assigned to the partition, where SecOC module is assigned to (via an EcucPduDedicatedPartition per PDU connected to SecOC module). By doing so there is no core affinity between the SecOC and the rest of the Com-Stack, because PduR dispatches the context to/from SecOC to the other modules.
In this case the SecOC module could be deployed on the “Crypto-Stack core”, no matter where the Com-Stack is deployed.

A multi instantiation of SecOC itself is not supported.

7.8 Error Classification

7.8.1 Development Errors

[SWS_SecOC_00101] Development Error Types
⌈

Type or error	*Related error code*	*Value [hex]*
An API service was called with a NULL pointer	SECOC_E_PARAM_POINTER	0x01
API service used without module initialization	SECOC_E_UNINIT	0x02
Invalid I-PDU	SECOC_E_INVALID_PDU_SDU_ID	0x03

identifier		
initialization of SecOC failed	SECOC_E_INIT_FAILED	0x07
Crypto service failed	SECOC_E_CRYPTO_FAILURE	0x04

] (SRS_BSW_00337, SRS_BSW_00385, SRS_BSW_00386)

7.8.2 Runtime Errors

[SWS_SecOC_00114] Runtime Error Types
[

Type or error	*Related error code*	*Value [hex]*
NO freshness value available from the Freshness Manager	SECOC_E_FRESHNESS_FAILURE	0x08

] (SRS_BSW_00337, SRS_BSW_00385, SRS_BSW_00386)

7.8.3 Transient Faults

There are no transient faults.

7.8.4 Production Errors

There are no production errors.

7.8.5 Extended Production Errors

There are no extended production errors.

7.9 Error detection

The detection of development errors is configurable (see Section 10.2, SecOcDevErrorDetect).

7.10 Error notification

The SecOC module checks the initialization state when one of its API functions is called, and reports the DET error SECOC_E_UNINIT in case an API call other than SecOC_Init or SecOC_GetVersionInfo occurs. If the initialization of the SecOC failed, the SecOC module reports the DET error SECOC_E_INIT_FAILED.Besides this, the SecOC module performs parameter checks for all called APIs. It reports the DET error SECOC_E_PARAM_POINTER when a call provides a NULL pointer and SECOC_E_INVALID_PDU_SDU_ID when a check

of aI-PDU ID fails. It reports SECOC_E_CRYPTO_FAILURE when the use of CSM function finally lead to a situation that PDUs can't be authenticated or.

[SWS_SecOC_00102]⌈
If DET reporting is enabled via SecOCDevErrorDetect and if the SecOC module has not been initialized, all functions except SecOC_Init and SecOC_GetVersionInfo shall report the error SECOC_E_UNINIT.
⌋ (SRS_BSW_00337, SRS_BSW_00350, SRS_BSW_00385, SRS_BSW_00450)

[SWS_SecOC_00164]⌈
If DET reporting is enabled via SecOCDevErrorDetect, the SecOC module shall check the I-PDU Id parameters of its API functions against its configuration and shall report the DET error SECOC_E_INVALID_PDU_SDU_ID when an unknown I-PDU Id is referenced by the call.
⌋ (SRS_BSW_00337, SRS_BSW_00350, SRS_BSW_00385)

[SWS_SecOC_00166]⌈
If DET reporting is enabled via SecOCDevErrorDetect, the SecOC module shall report the DET error SECOC_E_CRYPTO_FAILURE when it is finally not able to get the required security services for authentication/verification from the CSM.
⌋ (SRS_BSW_00337, SRS_BSW_00350,SRS_BSW_00385)

[SWS_SecOC_00251]⌈

The SecOC module shall report the DET error SECOC_E_RE_FRESHNESS_FAILURE when it is finally not able to get the required freshness services for authentication/verification from the Freshness Manager.

⌋ (SRS_SecOC_00022, SRS_SecOC_00029)

7.11 Security Profiles

7.11.1 Secured area within a Pdu

[SWS_SecOC_00311]⌈If the parameter SecOCSecuredTxPduOffset or SecOCSecuredRxPduOffset is available, the applied Security Profile shall only consider the bytes starting with the configured offset.⌋()

[SWS_SecOC_00312]⌈If the parameter SecOCSecuredTxPduLength or SecOCSecuredRxPduLength is available, the applied Security Profile shall only consider the configured length. ⌋()

[SWS_SecOC_00313]⌈If the sum of configured value of SecOCSecuredTxPduLength and SecOCSecuredTxPduOffset is longer than the PduInfoPtr->SduLength provided to SecOC_IfTransmit or SecOC_TpTransmit, this Pdu shall be discarded and E_NOT_OK shall be returned.⌋()

[SWS_SecOC_00314]⌈If the sum of configured value of SecOCSecuredRxPduLength and SecOCSecuredRxPduOffset are longer than the received Pdu length itself, this Pdu shall be discarded.⌋()

7.11.2 Overview of security profiles

The specification of the module Secure Onboard Communication allows different configurations for which cryptographic algorithms and modes to use for the MAC calculation and how the truncation of the MAC and freshness value (if applicable) shall be done. The security profiles provide a consistent set of values for a subset of configuration parameters that are relevant for the configuration of Secure Onboard Communication.

[SWS_SecOC_00190]⌈
Each Security Profile shall provide the configuration values for the authentication algorithm (parameter `algorithmFamily`, `algorithmMode` and `algorithmSecondaryFamily` in `CryptoServicePrimitive`), length of freshness Value, if applicable (parameter `SecOCFreshnessValueLength`), length of truncated Freshness Value (parameter `SecOCFreshnessValueTruncLength`), length of truncated MAC (parameter `SecOCAuthInfoTruncLength`), and a description of the profile.
⌋(SRS_SecOC_00003)

[SWS_SecOC_00191]⌈
A security profile shall be defined by the following mandatory parameters in the System Template:

+ algorithmFamily:String [0..1]
+ algorithmMode :String [0..1]
+ algorithmSecondaryFamily :String [0..1]
+ authInfoTxLength :PositiveInteger
+ freshnessValueLength :PositiveInteger
+ freshnessValueTruncLength :PositiveInteger

⌋(SRS_SecOC_00003)

7.11.3 SecOC Profile 1 (or 24Bit-CMAC-8Bit-FV)

[SWS_SecOC_00192]⌈
Using the CMAC algorithm based on AES-128 according to NIST SP 800-38B to calculate the MAC, use the eight least significant bit of the freshness value as truncated freshness value and use the 24 most significant bits of the MAC as truncated MAC.
⌋(SRS_SecOC_00003)

Parameter	*Configuration value*

The algorithm for the MAC (parameter `algorithmFamily`)	CRYPTO_ALGOFAM_AES
The algorithm mode for the MAC (parameter `algorithmMode`)	CRYPTO_ALGOMODE_CMAC
Additional algorithm family configuration (parameter `algorithmSecondaryFamily`, not used in this profile)	CRYPTO_ALGOFAM_NOT_SET
Length of Freshness Value (parameter `SecOCFreshnessValueLength`)	Not Specified
length of truncated Freshness Value (parameter `SecOCFreshnessValueTruncLength`	8 bits
length of truncated MAC (parameter `SecOCAuthInfoTruncLength`)	24 bits

7.11.4 SecOC Profile 2 (or 24Bit-CMAC-No-FV)

[SWS_SecOC_00193]⌈
Using the CMAC algorithm based on AES-128 according to NIST SP 800-38B to calculate the MAC, don't use any freshness value at all and use the 24 most significant bits of the MAC as truncated MAC.
The profile shall only be used if no synchronized freshness value is established. There is no restriction to a special bus.
⌋(SRS_SecOC_00003)

Parameter	*Configuration value*
The algorithm for the MAC (parameter `algorithmFamily`)	CRYPTO_ALGOFAM_AES
The algorithm mode for the MAC (parameter `algorithmMode`)	CRYPTO_ALGOMODE_CMAC
Additional algorithm family configuration (parameter `algorithmSecondaryFamily`, not used in this profile)	CRYPTO_ALGOFAM_NOT_SET
Length of Freshness Value (parameter `SecOCFreshnessValueLength`)SecOC	0
length of truncated Freshness Value (parameter `SecOCFreshnessValueTruncLength`	0 bits
length of truncated MAC (parameter `SecOCAuthInfoTruncLength`)	24 bits

7.11.5 SecOC Profile 3 (or JASPAR)

[SWS_SecOC_00194]⌈
This profile depicts one configuration and usage of the JasPar counter base FV with Master-Slave Synchronization method.
It uses the CMAC algorithm based on AES-128 according to NIST SP 800-38B Appendix-A to calculate the MAC. Use the 4 least significant bits of the freshness value as truncated freshness value and use the 28 most significant bits of the MAC as truncated MAC.
Freshness Value provided to SecOC shall be constructed as described in the [UC_SecOC_00202]. The profile shall be used for CAN.

](SRS_SecOC_00003)

Parameter	*Configuration value*
The algorithm for the MAC (parameter `algorithmFamily`)	CRYPTO_ALGOFAM_AES
The algorithm mode for the MAC (parameter `algorithmMode`)	CRYPTO_ALGOMODE_CMAC
Additional algorithm family configuration (parameter `algorithmSecondaryFamily`, not used in this profile)	CRYPTO_ALGOFAM_NOT_SET
Length of Freshness Value (parameter `SecOCFreshnessValueLength`)	64 bits
length of truncated Freshness Value (parameter `SecOCFreshnessValueTruncLength`	4 bits
length of truncated MAC (parameter `SecOCAuthInfoTruncLength`)	28 bits

8 API specification

8.1 Imported types

In this chapter, all types included from the following modules are listed:

[SWS_SecOC_00103]⌈

Module	*Header File*	*Imported Type*
ComStack_Types	ComStack_Types.h	BufReq_ReturnType
	ComStack_Types.h	PduIdType
	ComStack_Types.h	PduInfoType
	ComStack_Types.h	PduLengthType
	ComStack_Types.h	RetryInfoType
	ComStack_Types.h	TpDataStateType
Csm	Rte_Csm_Type.h	Crypto_OperationModeType
	Rte_Csm_Type.h	Crypto_VerifyResultType
Std	Std_Types.h	Std_ReturnType
	Std_Types.h	Std_VersionInfoType

⌋(SRS_BSW_00301)

8.2 Type definitions

8.2.1 SecOC_ConfigType

[SWS_SecOC_00104]⌈

Name	SecOC_ConfigType	
Kind	Structure	
Elements	implementation specific	
	Type	--
	Comment	The content of the configuration data structure is implementation specific.
Description	Configuration data structure of SecOC module	
Available via	SecOC.h	

⌋(SRS_SecOC_00001, SRS_SecOC_00003)

8.2.2 SecOC_StateType

[SWS_SecOC_00162][

Name	SecOC_StateType		
Kind	Enumeration		
Range	SECOC_UNINIT	--	SecOC module is not initialized
	SECOC_INIT	--	SecOC module is initialized
Description	States of the SecOC module		
Available via	SecOC.h		

](SRS_SecOC_00005)

8.3 Function definitions

8.3.1 SecOC_Init

[SWS_SecOC_00106][

Service Name	SecOC_Init	

Syntax	`void SecOC_Init (`
	`  const SecOC_ConfigType* config`
	`)`	

Service ID [hex]	0x01	
Sync/Async	Synchronous	
Reentrancy	Non Reentrant	
Parameters (in)	config	Pointer to a selected configuration structure
Parameters (inout)	None	
Parameters (out)	None	
Return value	None	
Description	Initializes the the SecOC module. Successful initialization leads to state Sec OC_INIT.	
Available via	SecOC.h	

](SRS_BSW_00101, SRS_BSW_00323, SRS_BSW_00358, SRS_BSW_00359, SRS_BSW_00414, , SRS_SecOC_00006)

8.3.2 SecOC_DeInit

[SWS_SecOC_00161]⌈

Service Name	SecOC_DeInit

Syntax	`void SecOC_DeInit (`
	`  void`
	`)`

Service ID [hex]	0x05
Sync/Async	Synchronous
Reentrancy	Non Reentrant
Parameters (in)	None
Parameters (inout)	None
Parameters (out)	None
Return value	None
Description	This service stops the secure onboard communication. All buffered I-PDU are removed and have to be obtained again, if needed, after SecOC_Init has been called. By a call to SecOC_DeInit the AUTOSAR SecOC module is put into a not initialized state (SecOC_UNINIT).
Available via	SecOC.h

⌋(SRS_BSW_00323, SRS_BSW_00359, SRS_SecOC_00006, SRS_SecOC_00020)

[SWS_SecOC_00157]⌈
Within `SecOC_DeInit` the module shall clear all internal global variables and the buffers of the SecOC I-PDUs.
⌋ (SRS_BSW_00323, SRS_SecOC_00006)

8.3.3 SecOC_GetVersionInfo

[SWS_SecOC_00107]⌈

Service Name	SecOC_GetVersionInfo

Syntax	`void SecOC_GetVersionInfo (`
	`  Std_VersionInfoType* versioninfo`
	`)`

Service ID [hex]	0x02
Sync/Async	Synchronous

Reentrancy	Reentrant	
Parameters (in)	None	
Parameters (inout)	None	
Parameters (out)	versioninfo	Pointer to where to store the version information of this module.
Return value	None	
Description	Returns the version information of this module.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00359, SRS_BSW_00407, SRS_BSW_00369, SRS_BSW_00003, SRS_BSW_00402)

8.3.4 SecOC_IfTransmit

[SWS_SecOC_00112][

Service Name	SecOC_IfTransmit	
Syntax	`Std_ReturnType SecOC_IfTransmit ( PduIdType TxPduId, const PduInfoType* PduInfoPtr )`	
Service ID [hex]	0x49	
Sync/Async	Synchronous	
Reentrancy	Reentrant for different PduIds. Non reentrant for the same PduId.	
Parameters (in)	TxPduId	Identifier of the PDU to be transmitted
	PduInfoPtr	Length of and pointer to the PDU data and pointer to Meta Data.
Parameters (inout)	None	
Parameters (out)	None	
Return value	Std_Return-Type	E_OK: Transmit request has been accepted. E_NOT_OK: Transmit request has not been accepted.
Description	Requests transmission of a PDU.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00357, SRS_BSW_00369, SRS_BSW_00449)
For detailed description, see Section 7.4.

8.3.5 SecOC_TpTransmit

[SWS_SecOC_91008]⌈

Service Name	SecOC_TpTransmit	
Syntax	`Std_ReturnType SecOC_TpTransmit ( PduIdType TxPduId, const PduInfoType* PduInfoPtr )`	
Service ID [hex]	0x49	
Sync/Async	Synchronous	
Reentrancy	Reentrant for different PduIds. Non reentrant for the same PduId.	
Parameters (in)	TxPduId	Identifier of the PDU to be transmitted
	PduInfoPtr	Length of and pointer to the PDU data and pointer to Meta Data.
Parameters (inout)	None	
Parameters (out)	None	
Return value	Std_Return-Type	E_OK: Transmit request has been accepted. E_NOT_OK: Transmit request has not been accepted.
Description	Requests transmission of a PDU.	
Available via	SecOC.h	

⌋(SRS_BSW_00323, SRS_BSW_00357, SRS_BSW_00369, SRS_BSW_00449)
For detailed description, see Section 7.4.

8.3.6 SecOC_IfCancelTransmit

[SWS_SecOC_00113]⌈

Service Name	SecOC_IfCancelTransmit	
Syntax	`Std_ReturnType SecOC_IfCancelTransmit ( PduIdType TxPduId )`	
Service ID [hex]	0x4a	
Sync/Async	Synchronous	
Reentrancy	Reentrant for different PduIds. Non reentrant for the same PduId.	
Parameters (in)	TxPduId	Identification of the PDU to be cancelled.
Parameters (inout)	None	

Parameters (out)	None	
Return value	Std_Return-Type	E_OK: Cancellation was executed successfully by the destination module. E_NOT_OK: Cancellation was rejected by the destination module.
Description	Requests cancellation of an ongoing transmission of a PDU in a lower layer communication module.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00357, SRS_BSW_00449, SRS_SecOC_00012)

8.3.7 SecOC_TpCancelTransmit

[SWS_SecOC_91009][

Service Name	SecOC_TpCancelTransmit	
Syntax	`Std_ReturnType SecOC_TpCancelTransmit ( PduIdType TxPduId )`	
Service ID [hex]	0x4a	
Sync/Async	Synchronous	
Reentrancy	Reentrant for different PduIds. Non reentrant for the same PduId.	
Parameters (in)	TxPduId	Identification of the PDU to be cancelled.
Parameters (inout)	None	
Parameters (out)	None	
Return value	Std_Return-Type	E_OK: Cancellation was executed successfully by the destination module. E_NOT_OK: Cancellation was rejected by the destination module.
Description	Requests cancellation of an ongoing transmission of a PDU in a lower layer communication module.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00357, SRS_BSW_00449, SRS_SecOC_00012)

8.3.8 SecOC_TpCancelReceive

[SWS_SecOC_91010][

Service Name	SecOC_TpCancelReceive	
Syntax	`Std_ReturnType SecOC_TpCancelReceive ( PduIdType RxPduId )`	
Service ID [hex]	0x4c	
Sync/Async	Synchronous	
Reentrancy	Non Reentrant	
Parameters (in)	RxPduId	Identification of the PDU to be cancelled.
Parameters (inout)	None	
Parameters (out)	None	
Return value	Std_Return-Type	E_OK: Cancellation was executed successfully by the destination module. E_NOT_OK: Cancellation was rejected by the destination module.
Description	Requests cancellation of an ongoing reception of a PDU in a lower layer transport protocol module.	
Available via	SecOC.h	

]()

8.3.9 Optional Interfaces

This chapter defines all external interfaces that are required to fulfil an optional functionality of the module.

[SWS_SecOC_00122]⌈

Service Name	SecOC_VerifyStatusOverride	
Syntax	`Std_ReturnType SecOC_VerifyStatusOverride ( uint16 ValueID, SecOC_OverrideStatusType overrideStatus, uint8 numberOfMessagesToOverride )`	
Service ID [hex]	0x0b	
Sync/Async	Synchronous	
Reentrancy	Non Reentrant for the same FreshnessValueID. Reentrant for different Freshness ValueIDs	
Parameters	ValueID	If SecOCOverrideStatusWithDataId is configured to FALSE, ValueID

(in)		is the ID of the Freshness Value used to control the verification behaviour of all assigned Secured I-PDUs according to the override Status. If SecOCOverrideStatusWithDataId is configured to TRUE, ValueID is the DataID of a Secured I-PDU that shall be controlled by the overrideStatus.
	override Status	Defines whether verification is executed and whether the I-PDU is passed on, and for how long the override is active.
	numberOf MessagesTo Override	Number of sequential verification to override when using a specific counter for authentication verification. This is only considered when OverrideStatus is equal to SECOC_OVERRIDE_DROP_UNTIL_ LIMIT, SECOC_OVERRIDE_SKIP_UNTIL_LIMIT or SECOC_ OVERRIDE_PASS_UNTIL_LIMIT.
Parameters (inout)	None	
Parameters (out)	None	
Return value	Std_Return-Type	E_OK: request successful E_NOT_OK: request failed
Description	This service provides the ability to force specific behaviour of SecOc: accept or drop an I-PDU with or without performing the verification of authenticator or independent of the authenticator verification result, and to force a specific result for SecOC_ VerificationResultType allowing additional fault handling in the application. Option SECOC_OVERRIDE_PASS_UNTIL_NOTICE, SECOC_OVERRIDE_SKIP_UNTIL_ LIMIT, SECOC_OVERRIDE_PASS_UNTIL_LIMIT or SECOC_OVERRIDE_SKIP_ UNTIL_NOTICE are available only if SecOCEnableForcedPassOverride is set to TRUE.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00357, SRS_BSW_00449, SRS_SecOC_00017)

[SWS_SecOC_91013][

Service Name	SecOC_SendDefaultAuthenticationInformation	
Syntax	`Std_ReturnType SecOC_SendDefaultAuthenticationInformation ( uint16 FreshnessValueID, boolean sendDefaultAuthenticationInformation )`	
Service ID [hex]	0x04	
Sync/Async	Synchronous	
Reentrancy	Non Reentrant for the same FreshnessValueID. Reentrant for different Freshness ValueIDs	
Parameters (in)	FreshnessValueID	ID of the Freshness Value for which sending SecOCDefault AuthenticationInformationPattern should be enabled.

	sendDefault Authentication Information	FALSE - sending SecOCDefaultAuthenticationInformation Pattern shall be disabled for given FreshnessValueID TRUE - sending SecOCDefaultAuthenticationInformationPattern shall be enabled for given FreshnessValueID
Parameters (inout)	None	
Parameters (out)	None	
Return value	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed
Description	The service provides the ability to enable the sending of un-authenticated PDU to lower layer. (example: in case authentication build counter has reached the configuration value SecOCAuthenticationBuildAttempts or the query of the freshness function returns E_NOT_OK or the calculation of the authenticator has returned a non-recoverable error such as returning E_NOT_OK or KEY_FAILURE). This service is optional (the service is available only if SecOCDefaultAuthenticationInformation Pattern is configured). If the service is not available or the service is available but the service was called with sendDefaultAuthenticationInformation as FALSE for a given FreshnessValueID , SecOC module shall remove the Authentic I-PDU from its internal buffer and cancel the transmission request in case the building of authentication Information failed. If the service is available and the service was called with sendDefaultAuthenticationInformation as TRUE for a given FreshnessValueID , SecOc will use SecOCDefaultAuthenticationInformationPattern as authentication Information and will not cancel the transmission request.	
Available via	SecOC.h	

](SRS_SecOC_00021)

8.4 Call-back notifications

8.4.1 SecOC_RxIndication

[SWS_SecOC_00124][

Service Name	SecOC_RxIndication	

Syntax	`void SecOC_RxIndication (`
	`  PduIdType RxPduId,`
	`  const PduInfoType* PduInfoPtr`
	`)`	

Service ID [hex]	0x42	
Sync/Async	Synchronous	
Reentrancy	Reentrant for different PduIds. Non reentrant for the same PduId.	
Parameters (in)	RxPduId	ID of the received PDU.
	Pdu	Contains the length (SduLength) of the received PDU, a pointer to a

	InfoPtr	buffer (SduDataPtr) containing the PDU, and the MetaData related to this PDU.
Parameters (inout)	None	
Parameters (out)	None	
Return value	None	
Description	Indication of a received PDU from a lower layer communication interface module.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00359, SRS_SecOC_00012)

8.4.2 SecOC_TpRxIndication

[SWS_SecOC_00125][

Service Name	SecOC_TpRxIndication	
Syntax	`void SecOC_TpRxIndication ( PduIdType id, Std_ReturnType result )`	
Service ID [hex]	0x45	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	id	Identification of the received I-PDU.
	result	Result of the reception.
Parameters (inout)	None	
Parameters (out)	None	
Return value	None	
Description	Called after an I-PDU has been received via the TP API, the result indicates whether the transmission was successful or not.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00359, SRS_BSW_00449, SRS_SecOC_00012)

8.4.3 SecOC_TxConfirmation

[SWS_SecOC_00126][

Service Name	SecOC_TxConfirmation	
Syntax	`void SecOC_TxConfirmation ( PduIdType TxPduId, Std_ReturnType result )`	
Service ID [hex]	0x40	
Sync/Async	Synchronous	
Reentrancy	Reentrant for different PduIds. Non reentrant for the same PduId.	
Parameters (in)	TxPduId	ID of the PDU that has been transmitted.
	result	E_OK: The PDU was transmitted. E_NOT_OK: Transmission of the PDU failed.
Parameters (inout)	None	
Parameters (out)	None	
Return value	None	
Description	The lower layer communication interface module confirms the transmission of a PDU, or the failure to transmit a PDU.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00359, SRS_SecOC_00012)

8.4.4 SecOC_TpTxConfirmation

[SWS_SecOC_00152][

Service Name	SecOC_TpTxConfirmation	
Syntax	`void SecOC_TpTxConfirmation ( PduIdType id, Std_ReturnType result )`	
Service ID [hex]	0x48	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	id	Identification of the transmitted I-PDU.
	result	Result of the transmission of the I-PDU.
Parameters (inout)	None	
Parameters	None	

(out)	
Return value	None
Description	This function is called after the I-PDU has been transmitted on its network, the result indicates whether the transmission was successful or not.
Available via	SecOC.h

](SRS_BSW_00323, SRS_BSW_00359, SRS_BSW_00449, SRS_SecOC_00012)

8.4.5 SecOC_TriggerTransmit

[SWS_SecOC_00127][

Service Name	SecOC_TriggerTransmit	
Syntax	`Std_ReturnType SecOC_TriggerTransmit ( PduIdType TxPduId, PduInfoType* PduInfoPtr )`	
Service ID [hex]	0x41	
Sync/Async	Synchronous	
Reentrancy	Reentrant for different PduIds. Non reentrant for the same PduId.	
Parameters (in)	TxPduId	ID of the SDU that is requested to be transmitted.
Parameters (inout)	PduInfoPtr	Contains a pointer to a buffer (SduDataPtr) to where the SDU data shall be copied, and the available buffer size in SduLengh. On return, the service will indicate the length of the copied SDU data in SduLength.
Parameters (out)	None	
Return value	Std_-Return-Type	E_OK: SDU has been copied and SduLength indicates the number of copied bytes. E_NOT_OK: No SDU data has been copied. PduInfoPtr must not be used since it may contain a NULL pointer or point to invalid data.
Description	Within this API, the upper layer module (called module) shall check whether the available data fits into the buffer size reported by PduInfoPtr->SduLength. If it fits, it shall copy its data into the buffer provided by PduInfoPtr->SduDataPtr and update the length of the actual copied data in PduInfoPtr->SduLength. If not, it returns E_ NOT_OK without changing PduInfoPtr.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00357, SRS_BSW_00449, SRS_SecOC_00012)

8.4.6 SecOC_CopyRxData

[SWS_SecOC_00128][

Service Name	SecOC_CopyRxData	
Syntax	`BufReq_ReturnType SecOC_CopyRxData ( PduIdType id, const PduInfoType* info, PduLengthType* bufferSizePtr )`	
Service ID [hex]	0x44	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	id	Identification of the received I-PDU.
	info	Provides the source buffer (SduDataPtr) and the number of bytes to be copied (SduLength). An SduLength of 0 can be used to query the current amount of available buffer in the upper layer module. In this case, the SduDataPtr may be a NULL_PTR.
Parameters (inout)	None	
Parameters (out)	bufferSizePtr	Available receive buffer after data has been copied.
Return value	BufReq_-Return-Type	BUFREQ_OK: Data copied successfully BUFREQ_E_NOT_OK: Data was not copied because an error occurred.
Description	This function is called to provide the received data of an I-PDU segment (N-PDU) to the upper layer. Each call to this function provides the next part of the I-PDU data. The size of the remaining buffer is written to the position indicated by bufferSizePtr.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00357, SRS_SecOC_00012)

8.4.7 SecOC_CopyTxData

[SWS_SecOC_00129][

Service Name	SecOC_CopyTxData
Syntax	`BufReq_ReturnType SecOC_CopyTxData ( PduIdType id, const PduInfoType* info, const RetryInfoType* retry, PduLengthType* availableDataPtr )`

Service ID [hex]	0x43	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	id	Identification of the transmitted I-PDU.
	info	Provides the destination buffer (SduDataPtr) and the number of bytes to be copied (SduLength). If not enough transmit data is available, no data is copied by the upper layer module and BUFREQ_E_BUSY is returned. The lower layer module may retry the call. An SduLength of 0 can be used to indicate state changes in the retry parameter or to query the current amount of available data in the upper layer module. In this case, the SduDataPtr may be a NULL_PTR.
	retry	This parameter is used to acknowledge transmitted data or to retransmit data after transmission problems. If the retry parameter is a NULL_PTR, it indicates that the transmit data can be removed from the buffer immediately after it has been copied. Otherwise, the retry parameter must point to a valid RetryInfoType element. If TpDataState indicates TP_CONFPENDING, the previously copied data must remain in the TP buffer to be available for error recovery. TP_DATACONF indicates that all data that has been copied before this call is confirmed and can be removed from the TP buffer. Data copied by this API call is excluded and will be confirmed later. TP_DATARETRY indicates that this API call shall copy previously copied data in order to recover from an error. In this case TxTpDataCnt specifies the offset in bytes from the current data copy position.
Parameters (inout)	None	
Parameters (out)	available DataPtr	Indicates the remaining number of bytes that are available in the upper layer module's Tx buffer. availableDataPtr can be used by TP modules that support dynamic payload lengths (e.g. FrIsoTp) to determine the size of the following CFs.
Return value	BufReq_-Return-Type	BUFREQ_OK: Data has been copied to the transmit buffer completely as requested. BUFREQ_E_BUSY: Request could not be fulfilled, because the required amount of Tx data is not available. The lower layer module may retry this call later on. No data has been copied. BUFREQ_E_NOT_OK: Data has not been copied. Request failed.
Description	This function is called to acquire the transmit data of an I-PDU segment (N-PDU). Each call to this function provides the next part of the I-PDU data unless retry->Tp DataState is TP_DATARETRY. In this case the function restarts to copy the data beginning at the offset from the current position indicated by retry->TxTpDataCnt. The size of the remaining data is written to the position indicated by availableDataPtr.	
Available via	SecOC.h	

](SRS_BSW_00323, SRS_BSW_00357, SRS_SecOC_00012)

8.4.8 SecOC_StartOfReception

[SWS_SecOC_00130]⌈

Service Name	SecOC_StartOfReception	

Syntax	`BufReq_ReturnType SecOC_StartOfReception (`
	`  PduIdType id,`
	`  const PduInfoType* info,`
	`  PduLengthType TpSduLength,`
	`  PduLengthType* bufferSizePtr`
	`)`	

Service ID [hex]	0x46	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	id	Identification of the I-PDU.
	info	Pointer to a PduInfoType structure containing the payload data (without protocol information) and payload length of the first frame or single frame of a transport protocol I-PDU reception, and the MetaData related to this PDU. If neither first/single frame data nor MetaData are available, this parameter is set to NULL_PTR.
	TpSdu Length	Total length of the N-SDU to be received.
Parameters (inout)	None	
Parameters (out)	buffer SizePtr	Available receive buffer in the receiving module. This parameter will be used to compute the Block Size (BS) in the transport protocol module.
Return value	BufReq_- Return- Type	BUFREQ_OK: Connection has been accepted. bufferSizePtr indicates the available receive buffer; reception is continued. If no buffer of the requested size is available, a receive buffer size of 0 shall be indicated by bufferSizePtr. BUFREQ_E_NOT_OK: Connection has been rejected; reception is aborted. bufferSizePtr remains unchanged. BUFREQ_E_OVFL: No buffer of the required length can be provided; reception is aborted. bufferSizePtr remains unchanged.
Description	This function is called at the start of receiving an N-SDU. The N-SDU might be fragmented into multiple N-PDUs (FF with one or more following CFs) or might consist of a single N-PDU (SF). The service shall provide the currently available maximum buffer size when invoked with TpSduLength equal to 0.	
Available via	SecOC.h	

⌋(SRS_BSW_00323, SRS_BSW_00357, SRS_SecOC_00012)

[SWS_SecOC_00181] ⌈
In case `SecOC_StartOfReception`is called with `TpSduLength`equal to 0, the SecOC module shall return `BUFREQ_E_NOT_OK` and no further action shall be taken.

] ()

8.4.9 CSM callback interfaces

[SWS_SecOC_00012] [
If the SecOC module uses the Csm module asynchronously to calculate or verify the authenticator, SecOC shall provide callback functions according to `Csm_CallbackType`.
] (SRS_BSW_00457, SRS_SecOC_00003)

8.5 Callout Definitions

Callouts are pieces of code that have to be added to the SecOC during ECU integration. The content of most callouts is hand-written code.

8.5.1 SecOC_GetRxFreshness

[SWS_SecOC_91007][

Service Name	SecOC_GetRxFreshness	

Syntax	`Std_ReturnType SecOC_GetRxFreshness (`
	`  uint16 SecOCFreshnessValueID,`
	`  const uint8* SecOCTruncatedFreshnessValue,`
	`  uint32 SecOCTruncatedFreshnessValueLength,`
	`  uint16 SecOCAuthVerifyAttempts,`
	`  uint8* SecOCFreshnessValue,`
	`  uint32* SecOCFreshnessValueLength`
	`)`	

Service ID [hex]	0x4f	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	SecOCFreshness ValueID	Holds the identifier of the freshness value.
	SecOCTruncated FreshnessValue	Holds the truncated freshness value that was contained in the Secured I-PDU.
	SecOCTruncated FreshnessValue Length	Holds the length in bits of the truncated freshness value.
	SecOCAuthVerify Attempts	Holds the number of authentication verify attempts of this PDU since the last reception. The value is 0 for the first attempt and incremented on every unsuccessful verification attempt.
Parameters (inout)	SecOCFreshness ValueLength	Holds the length in bits of the freshness value.

Parameters (out)	SecOCFreshness Value	Holds the freshness value to be used for the calculation of the authenticator.
Return value	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed, a freshness value cannot be provided due to general issues for freshness or this FreshnessValueId. E_BUSY: The freshness information can temporarily not be provided.
Description	This interface is used by the SecOC to obtain the current freshness value.	
Available via	SecOC.h	

](SRS_SECOC_00003)

8.5.2 SecOC_GetRxFreshnessAuthData

[SWS_SecOC_91006][

Service Name	SecOC_GetRxFreshnessAuthData	

Syntax	`Std_ReturnType SecOC_GetRxFreshnessAuthData (`
	`  uint16 SecOCFreshnessValueID,`
	`  const uint8* SecOCTruncatedFreshnessValue,`
	`  uint32 SecOCTruncatedFreshnessValueLength,`
	`  const uint8* SecOCAuthDataFreshnessValue,`
	`  uint16 SecOCAuthDataFreshnessValueLength,`
	`  uint16 SecOCAuthVerifyAttempts,`
	`  uint8* SecOCFreshnessValue,`
	`  uint32* SecOCFreshnessValueLength`
	`)`	

Service ID [hex]	0x4e	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	SecOCFreshness ValueID	Holds the identifier of the freshness value.
	SecOCTruncated FreshnessValue	Holds the truncated freshness value that was contained in the Secured I-PDU.
	SecOCTruncated FreshnessValue Length	Holds the length in bits of the truncated freshness value.
	SecOCAuthData FreshnessValue	The parameter holds a part of the received, not yet authenticated PDU. The parameter is optional (see description)
	SecOCAuthData FreshnessValue Length	This is the length value in bits that holds the freshness from the authentic PDU. The parameter is optional (see description).

	SecOCAuthVerify Attempts	Holds the number of authentication verify attempts of this PDU since the last reception. The value is 0 for the first attempt and incremented on every unsuccessful verification attempt.
Parameters (inout)	SecOCFreshness ValueLength	Holds the length in bits of the freshness value.
Parameters (out)	SecOCFreshness Value	Holds the freshness value to be used for the calculation of the authenticator.
Return value	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed, a freshness value cannot be provided due to general issues for freshness or this FreshnessValueId. E_BUSY: The freshness information can temporarily not be provided.
Description	This interface is used by the SecOC to obtain the current freshness value.	
Available via	SecOC.h	

](SRS_SECOC_00003)

8.5.3 SecOC_GetTxFreshness

[SWS_SecOC_91004][

Service Name	SecOC_GetTxFreshness	
Syntax	`Std_ReturnType SecOC_GetTxFreshness ( uint16 SecOCFreshnessValueID, uint8* SecOCFreshnessValue, uint32* SecOCFreshnessValueLength )`	
Service ID [hex]	0x52	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	SecOCFreshness ValueID	Holds the identifier of the freshness value.
Parameters (inout)	SecOCFreshness ValueLength	Holds the length of the provided freshness in bits.
Parameters (out)	SecOCFreshness Value	Holds the current freshness value
Return value	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed, a freshness value cannot be provided due to general issues for freshness or this FreshnessValueId. E_BUSY: The freshness information can temporarily not be

		provided.
Description	This API returns the freshness value from the Most Significant Bits in the first byte in the array (SecOCFreshnessValue), in big endian format.	
Available via	SecOC.h	

](SRS_SECOC_00003, SRS_SECOC_00006)

8.5.4 SecOC_GetTxFreshnessTruncData

[SWS_SecOC_91003][

Service Name	SecOC_GetTxFreshnessTruncData	
Syntax	`Std_ReturnType SecOC_GetTxFreshnessTruncData ( uint16 SecOCFreshnessValueID, uint8* SecOCFreshnessValue, uint32* SecOCFreshnessValueLength, uint8* SecOCTruncatedFreshnessValue, uint32* SecOCTruncatedFreshnessValueLength )`	
Service ID [hex]	0x51	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	SecOCFreshness ValueID	Holds the identifier of the freshness value.
Parameters (inout)	SecOCFreshness ValueLength	Holds the length of the provided freshness in bits.
	SecOCTruncated FreshnessValue Length	Provides the truncated freshness length configured for this freshness. The function may adapt the value if needed or can leave it unchanged if the configured length and provided length is the same.
Parameters (out)	SecOCFreshness Value	Holds the current freshness value.
	SecOCTruncated FreshnessValue	Holds the truncated freshness to be included into the Secured I-PDU. The parameter is optional.
Return value	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed, a freshness value cannot be provided due to general issues for freshness or this FreshnessValueId. E_BUSY: The freshness information can temporarily not be provided.
Description	This interface is used by the SecOC to obtain the current freshness value. The interface function provides also the truncated freshness transmitted in the secured I-	

	PDU.
Available via	SecOC.h

](SRS_SECOC_00003, SRS_SECOC_00006)

8.5.5 SecOC_SPduTxConfirmation

[SWS_SecOC_91005][

Service Name	SecOC_SPduTxConfirmation	
Syntax	`void SecOC_SPduTxConfirmation ( uint16 SecOCFreshnessValueID )`	
Service ID [hex]	0x4d	
Sync/Async	Synchronous	
Reentrancy	Reentrant	
Parameters (in)	SecOCFreshnessValueID	Holds the identifier of the freshness value.
Parameters (inout)	None	
Parameters (out)	None	
Return value	None	
Description	This interface is used by the SecOC to indicate that the Secured I-PDU has been initiated for transmission.	
Available via	SecOC.h	

](SRS_SECOC_00002, SRS_SECOC_00003)

8.6 Scheduled functions

8.6.1 SecOC_MainFunctionRx

[SWS_SecOC_00171][

Service Name	SecOC_MainFunctionRx
Syntax	`void SecOC_MainFunctionRx ( void )`
Service ID [hex]	0x06

Description	This function performs the processing of the SecOC module's authentication and verification processing for the Rx path.
Available via	SchM_SecOC.h

](SRS_BSW_00373, SRS_BSW_00425)

[SWS_SecOC_00172][
If the SecOC module was not previously initialized with a call to `SecOC_Init`, then a call to `SecOC_MainFunctionRx` shall simply return.
] (SRS_SecOC_00005)

[SWS_SecOC_00173][
The cycle time of the `SecOC_MainFunctionRx` is configured by the parameter `SecOCMainFunctionPeriodRx`.
] (SRS_SecOC_00025)

[SWS_SecOC_00174][
If `SecOC_MainFunctionRx` is scheduled, the SecOC shall firstly check if there are new Secured I-PDUs to be verified. If yes the SecOC module shall process the verification of each of the IPDUs identified as new subsequently in the very same main function call.
] (SRS_SecOC_00025)

[SWS_SecOC_00175][
For each newly successfully verified Secured I-PDU, the SecOC module shall immediately pass the Authentic I-PDU to the upper layer communication module by calling `PduR_SecOC[If|Tp]RxIndication`for the Authentic I-PDU.
] (SRS_SecOC_00025)

8.6.2 SecOC_MainFunctionTx

[SWS_SecOC_00176][

Service Name	SecOC_MainFunctionTx

Syntax	`void SecOC_MainFunctionTx (`
	`  void`
	`)`

Service ID [hex]	0x03
Description	This function performs the processing of the SecOC module's authentication and verification processing for the Tx path.
Available via	SchM_SecOC.h

](SRS_BSW_00373, SRS_BSW_00425)

[SWS_SecOC_00177][

If the SecOC module was not previously initialized with a call to `SecOC_Init`, then a call to `SecOC_MainFunctionTx` shall simply return.
] (SRS_SecOC_00005)

[SWS_SecOC_00178][
The cycle time of the `SecOC_MainFunctionTx` is configured by the parameter `SecOCMainFunctionPeriodTx`.
] (SRS_SecOC_00025)

[SWS_SecOC_00179][
If `SecOC_MainFunctionTx` is scheduled, the SecOC shall firstly check if there are new Authentic I-PDUs to be authenticated. If yes the SecOC module shall process the authentication of each of the IPDUs identified as new subsequently in the very same main function call.
] (SRS_SecOC_00025)

[SWS_SecOC_00180][
For each newly authenticated Authentic I-PDU, the SecOC module shall immediately trigger the transmission of the Secured I-PDU at the lower layer module by calling the PduR.
] (SRS_SecOC_00025)

8.7 Expected Interfaces

8.7.1 Mandatory Interfaces

This chapter defines all external interfaces that are required to fulfill the core functionality of the module.

[SWS_SecOC_00137][

API Function	***Header File***	***Description***
Det_ReportRuntime-Error	Det.h	Service to report runtime errors. If a callout has been configured then this callout shall be called.
PduR_SecOC-CancelTransmit	PduR_SecOC.h	Requests cancellation of an ongoing transmission of a PDU in a lower layer communication module.
PduR_SecOCIfRx-Indication	PduR_SecOC.h	Indication of a received PDU from a lower layer communication interface module.
PduR_SecOCIfTx-Confirmation	PduR_SecOC.h	The lower layer communication interface module confirms the transmission of a PDU, or the failure to transmit a PDU.
PduR_SecOC-Transmit	PduR_SecOC.h	Requests transmission of a PDU.

](SRS_BSW_00384)

8.7.2 Optional Interfaces

[SWS_SecOC_00138]⌈

API Function	*Header File*	*Description*
Csm_Mac-Generate	Csm.h	Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer.
Csm_MacVerify	Csm.h	Verifies the given MAC by comparing if the MAC is generated with the given data.
Csm_Signature-Generate	Csm.h	Uses the given data to perform the signature calculation and stores the signature in the memory location pointed by the result pointer.
Csm_Signature-Verify	Csm.h	Verifies the given MAC by comparing if the signature is generated with the given data.
Det_Report-Error	Det.h	Service to report development errors.
PduR_SecOC-CancelReceive	PduR_SecOC.h	Requests cancellation of an ongoing reception of a PDU in a lower layer transport protocol module.
PduR_SecOC-TpCopyRxData	PduR_SecOC.h	This function is called to provide the received data of an I-PDU segment (N-PDU) to the upper layer. Each call to this function provides the next part of the I-PDU data. The size of the remaining buffer is written to the position indicated by bufferSizePtr.
PduR_SecOC-TpCopyTxData	PduR_SecOC.h	This function is called to acquire the transmit data of an I-PDU segment (N-PDU). Each call to this function provides the next part of the I-PDU data unless retry->TpDataState is TP_DATARETRY. In this case the function restarts to copy the data beginning at the offset from the current position indicated by retry->TxTpDataCnt. The size of the remaining data is written to the position indicated by availableDataPtr.
PduR_SecOC-TpRxIndication	PduR_SecOC.h	Called after an I-PDU has been received via the TP API, the result indicates whether the transmission was successful or not.
PduR_SecOC-TpStartOf-Reception	PduR_SecOC.h	This function is called at the start of receiving an N-SDU. The N-SDU might be fragmented into multiple N-PDUs (FF with one or more following CFs) or might consist of a single N-PDU (SF). The service shall provide the currently available maximum buffer size when invoked with TpSduLength equal to 0.
PduR_SecOC-TpTx-Confirmation	PduR_SecOC.h	This function is called after the I-PDU has been transmitted on its network, the result indicates whether the transmission was successful or not.

⌋(SRS_BSW_00384)

8.7.3 Configurable Interfaces

8.7.3.1 SecOC_VerificationStatusCallout

If configured by `SecOCVerificationStatusCallout` (see ECUC_SecOC_00004), the SecOC module shall invoke a callout function to notify other modules on the verification status of the most recently received Secured I-PDU.

[SWS_SecOC_00119][

Service Name	SecOC_VerificationStatusCallout	
Syntax	`void SecOC_VerificationStatusCallout ( SecOC_VerificationStatusType verificationStatus )`	
Service ID [hex]	0x50	
Sync/Async	Synchronous	
Reentrancy	Non Reentrant for the same FreshnessValueID. Reentrant for different Freshness ValueIDs	
Parameters (in)	verification Status	Data structure to bundle the status of a verification attempt for a specific Freshness Value and Data ID
Parameters (inout)	None	
Parameters (out)	None	
Return value	None	
Description	Service is used to propagate the status of each verification attempt from the Sec OC module to other modules. This service can be configured such that: • Only: "False" Verification Status is propagated to modules • Both: "True" and "False" Verification Status are propagated to modules • None: No Verification Status is propagated	
Available via	SecOC_Externals.h	

](SRS_BSW_00359, SRS_SecOC_00017)

Note: The argument `freshnessValueID` allows for unambiguously identifying the Secured I-PDU that was subject of the verification attempt. Since each Secured I-PDU has at least one but possibly two related Freshness Value IDs (i.e. a Secured I-PDU may have a Secondary Freshness Value ID), `SecOC_VerificationStatusCallout` is able to indicate for which of the freshness values the verification attempt has been carried out.

Note: Any module that is configured to be notified by the means of `SecOC_VerificationStatusCallout` has to implement a target function that is conforming to the above signature. The name of the target function listed above are not fixed. The name could be configured by means of the parameter `SecOCVerificationStatusCallout`.

8.8 Service Interfaces

This chapter defines the AUTOSAR Interfaces of the SecOC Service (<MA>).

The definitions in this section are interpreted to be in `ARPackage AUTOSAR/Services/<MA>`.

8.8.1 Overview

This chapter is an addition to the specification of the SecOC module. Whereas the other parts of the specification define the behavior and the C-interfaces of the corresponding basic software module, this chapter formally specifies the corresponding AUTOSAR service in terms of the SWC template. The interfaces described here will be visible on the VFB and are used to generate the Rte between application software and the SecOC module.

8.8.2 Sender Receiver Interfaces

8.8.2.1 Verification Status Service

[SWS_SecOC_00141]⌈

Name	VerificationStatus	
Comment	This service realizes a notification service that is used to propagate the status of each authentication attempt from the SecOC module to the application layer. This service can be configured such that: • Only "False" Verification Status is propagated to the application layer • Both "True" and "False" Verification Status are propagated to the application layer • No Verification Status is propagated to the application layer	
IsService	true	
Variation	--	
Data Elements	verificationStatus	
	Type	SecOC_VerificationStatusType
	Variation	--

⌋(SRS_SecOC_00022)

Note: The `SecOC_VerificationStatusService` is used to propagate the status of each verification attempt from the SecOC module to an arbitrary number of application software components. It can be used to continuously monitor the number of failed verification attempts and would allow setting up a security management system/intrusion detection system that is able to detect an attack flood and react with adequate dynamic countermeasures.

[SWS_SecOC_00148]⌈

SecOC shall define a provide port for the `SecOC_VerificationStatusService` interface and call the generated Rte function as configured by the parameter `SecOCVerificationStatusPropagationMode`. The sender/receiver interface shall be defined as standard interface.

](SRS_SecOC_00022)

8.8.3 Client Server Interfaces

8.8.3.1 Verification Status Configuration Service

[SWS_SecOC_00142][

Name	VerifyStatusConfiguration		
Comment	Verify Status Configuration Service of SecOC		
IsService	true		
Variation	--		
Possible Errors	0	E_OK	Operation successful
	1	E_NOT_OK	Operation failed

Operation	VerifyStatusOverride	
Comment	This service provides the ability to force specific behaviour of SecOc: accept or drop an I-PDU with or without performing the verification of authenticator or independent of the authenticator verification result, and to force a specific result for SecOC_ VerificationResultType allowing additional fault handling in the application. Option SECOC_OVERRIDE_PASS_UNTIL_NOTICE, SECOC_OVERRIDE_SKIP_ UNTIL_LIMIT, SECOC_OVERRIDE_PASS_UNTIL_LIMIT or SECOC_OVERRIDE_ SKIP_UNTIL_NOTICE are available only if SecOCEnableForcedPassOverride is set to TRUE.	
Variation	--	
Parameters	ValueId	
	Type	uint16
	Direction	IN
	Comment	Identifier of the Value ID where override shall be applied to. If configuration option SecOCOverrideStatusWithDataId is set to TRUE, this value shall provide the DataID of the secured I-PDU. If Sec OCOverrideStatusWithDataId is set to FALSE, this parameter shall provide the freshness value ID.
	Variation	--
	overrideStatus	
	Type	SecOC_OverrideStatusType
	Direction	IN
	Comment	Defines whether verification is executed and whether the I-PDU is

		passed on, and for how long the override is active.
	Variation	--
	numberOfMessagesToOverride	
	Type	uint8
	Direction	IN
	Comment	Number of sequential VerifyStatus to override when using a specific counter for authentication verification. This is only considered when OverrideStatus is equal to SECOC_OVERRIDE_DROP_UNTIL_LIMIT, SECOC_OVERRIDE_SKIP_UNTIL_LIMIT or SECOC_OVERRIDE_ PASS_UNTIL_LIMIT.
	Variation	--
Possible Errors	E_OK E_NOT_OK	

](SRS_SecOC_00017)

8.8.3.2 FreshnessManagement

[SWS_SecOC_91002][

Name	FreshnessManagement		
Comment	Freshness Management for SecOC		
IsService	true		
Variation	--		
Possible Errors	0	E_OK	Operation successful
	1	E_NOT_ OK	Operation failed
	2	E_BUSY	Operation temporary failed, a freshness cannot be provided at the moment.

Operation	GetRxFreshness	
Comment	This interface is used by the SecOC to obtain the current freshness value. This operation provides also a part of the Authentic-PDU data if configured.	
Variation	({ecuc(SecOC/SecOCRxPduProcessing/SecOCUseAuthDataFreshness)} == FALSE)	
Parameters	freshnessValueId	
	Type	uint16
	Direction	IN
	Comment	Identifier of the freshness

	Variation	--
	truncatedFreshnessValue	
	Type	SecOC_FreshnessArrayType
	Direction	IN
	Comment	The truncated freshness value from the received Secured-IPDU
	Variation	--
	truncatedFreshnessValueLength	
	Type	uint32
	Direction	IN
	Comment	Length in bits of the truncated freshness value
	Variation	--
	authVerifyAttempts	
	Type	uint16
	Direction	IN
	Comment	The number of authentication verify attempts for the current PDU
	Variation	--
	freshnessValue	
	Type	SecOC_FreshnessArrayType
	Direction	OUT
	Comment	The freshness value for this PDU
	Variation	--
	freshnessValueLength	
	Type	uint32
	Direction	INOUT
	Comment	The freshness value length in bits.
	Variation	--
Possible Errors	E_OK E_NOT_OK E_BUSY	

Operation	GetRxFreshnessAuthData
Comment	This interface is used by the SecOC to obtain the current freshness value. This operation provides also a part of the Authentic-PDU data if configured.

Variation	({ecuc(SecOC/SecOCRxPduProcessing/SecOCUseAuthDataFreshness)} == TRUE)	
Parameters	freshnessValueId	
	Type	uint16
	Direction	IN
	Comment	Identifier of the freshness
	Variation	--
	truncatedFreshnessValue	
	Type	SecOC_FreshnessArrayType
	Direction	IN
	Comment	The truncated freshness value from the received Secured-IPDU
	Variation	--
	truncatedFreshnessValueLength	
	Type	uint32
	Direction	IN
	Comment	Length in bits of the truncated freshness value
	Variation	--
	authenticDataFreshnessValue	
	Type	SecOC_FreshnessArrayType
	Direction	IN
	Comment	The selected part of the authentic data.
	Variation	--
	authenticDataFreshnessValueLength	
	Type	uint16
	Direction	IN
	Comment	The length in bits of the authentic data part.
	Variation	--
	authVerifyAttempts	
	Type	uint16
	Direction	IN
	Comment	The number of authentication verify attempts for this PDU
	Variation	--

	freshnessValue	
	Type	SecOC_FreshnessArrayType
	Direction	OUT
	Comment	The freshness value for this PDU
	Variation	--
	freshnessValueLength	
	Type	uint32
	Direction	INOUT
	Comment	The freshness value length in bits.
	Variation	--
Possible Errors	E_OK E_NOT_OK E_BUSY	

Operation	GetTxFreshness	
Comment	Returns the freshness value from the Most Significant Bits in the first byte in the array (SecOCFreshnessValue), in big endian format.	
Variation	({ecuc(SecOC/SecOCTxPduProcessing/SecOCProvideTxTruncatedFreshnessValue)} == FALSE)	
Parameters	freshnessValueId	
	Type	uint16
	Direction	IN
	Comment	Identifier of the freshness
	Variation	--
	freshnessValue	
	Type	SecOC_FreshnessArrayType
	Direction	OUT
	Comment	Freshness value
	Variation	--
	freshnessValueLength	
	Type	uint32
	Direction	INOUT
	Comment	Length in bits of the freshness value

	Variation	--
Possible Errors	E_OK E_NOT_OK E_BUSY	

Operation	GetTxFreshnessTruncData	
Comment	This operation is used by the SecOC to obtain the freshness that corresponds to the freshnessValueId. The operation provides the freshness and also the truncated freshness that shall be placed into the Secured-IPDU.	
Variation	({ecuc(SecOC/SecOCTxPduProcessing/SecOCProvideTxTruncatedFreshnessValue)} == TRUE)	
Parameters	freshnessValueId	
	Type	uint16
	Direction	IN
	Comment	Identifier of the freshness
	Variation	--
	freshnessValue	
	Type	SecOC_FreshnessArrayType
	Direction	OUT
	Comment	Freshness value
	Variation	--
	freshnessValueLength	
	Type	uint32
	Direction	INOUT
	Comment	Length in bits of the freshness value
	Variation	--
	truncatedFreshnessValue	
	Type	SecOC_FreshnessArrayType
	Direction	OUT
	Comment	The truncated freshness value that has to be placed into the Secured-IPDU
	Variation	--
	truncatedFreshnessValueLength	
	Type	uint32

	Direction	INOUT
	Comment	The length in bits for the truncated freshness.
	Variation	--
Possible Errors	E_OK E_NOT_OK E_BUSY	

Operation	SPduTxConfirmation	
Comment	This operation is used by the SecOC to indicate that the Secured I-PDU has been initiated for transmission.	
Variation	--	
Parameters	freshnessValueId	
	Type	uint16
	Direction	IN
	Comment	Identifier of the freshness
	Variation	--
Possible Errors	E_OK	

](SRS_SECOC_00003, SRS_SECOC_00021, SRS_SECOC_00022)

8.8.3.3 Sending Default Authentication Information configuration service [SWS_SecOC_00142]⌈

Name	VerifyStatusConfiguration		
Comment	Verify Status Configuration Service of SecOC		
IsService	true		
Variation	--		
Possible Errors	0	E_OK	Operation successful
	1	E_NOT_OK	Operation failed

Operation	VerifyStatusOverride
Comment	This service provides the ability to force specific behaviour of SecOc: accept or drop an I-PDU with or without performing the verification of authenticator or independent of the authenticator verification result, and to force a specific result for SecOC_ VerificationResultType allowing additional fault handling in the application. Option SECOC_OVERRIDE_PASS_UNTIL_NOTICE, SECOC_OVERRIDE_SKIP_ UNTIL_LIMIT, SECOC_OVERRIDE_PASS_UNTIL_LIMIT or SECOC_OVERRIDE_ SKIP_UNTIL_NOTICE are available only if SecOCEnableForcedPassOverride is set to TRUE.

Variation	--	
Parameters	ValueId	
	Type	uint16
	Direction	IN
	Comment	Identifier of the Value ID where override shall be applied to. If configuration option SecOCOverrideStatusWithDataId is set to TRUE, this value shall provide the DataID of the secured I-PDU. If Sec OCOverrideStatusWithDataId is set to FALSE, this parameter shall provide the freshness value ID.
	Variation	--
	overrideStatus	
	Type	SecOC_OverrideStatusType
	Direction	IN
	Comment	Defines whether verification is executed and whether the I-PDU is passed on, and for how long the override is active.
	Variation	--
	numberOfMessagesToOverride	
	Type	uint8
	Direction	IN
	Comment	Number of sequential VerifyStatus to override when using a specific counter for authentication verification. This is only considered when OverrideStatus is equal to SECOC_OVERRIDE_DROP_UNTIL_LIMIT, SECOC_OVERRIDE_SKIP_UNTIL_LIMIT or SECOC_OVERRIDE_ PASS_UNTIL_LIMIT.
	Variation	--
Possible Errors	E_OK E_NOT_OK	

⌋(SRS_SecOC_00017)

8.8.4 Ports

8.8.4.1 Freshness Management

[SWS_SecOC_91001]⌈

Name	FreshnessManagement		
Kind	RequiredPort	***Interface***	SendDefaultAuthenticationInformation
Description	Port for the provision of freshness for SecOC.		
Variation	({ecuc(SecOC/SecOCGeneral/SecOCQueryFreshnessValue)} == RTE)		

](SRS_SECOC_00003)

8.8.5 Implementation Data Types

8.8.5.1 SecOC_FreshnessArrayType [SWS_SecOC_91012]⌈

Name	SecOC_FreshnessArrayType		
Kind	Array	***Element type***	uint8
Size	SECOC_MAX_FRESHNESS_SIZE Elements		
Description	--		
Variation	--		
Available via	Rte_SecOC_Type.h		

](SRS_SECOC_00003, SRS_SECOC_00021, SRS_SECOC_00022)

8.8.5.2 SecOC_VerificationResultType [SWS_SecOC_00149]⌈

Name	SecOC_VerificationResultType		
Kind	Enumeration		
Range	SECOC_VERIFICATIONSUCCESS	0x00	Verification successful
	SECOC_VERIFICATIONFAILURE	0x01	Verification not successful
	SECOC_FRESHNESSFAILURE	0x02	Verification not successful because of wrong freshness value.
	SECOC_ AUTHENTICATIONBUILDFAILURE	0x03	Verification not successful because of wrong build authentication codes
	SECOC_NO_VERIFICATION	0x04	Verification has been skipped and the data has been provided to upper layer "as is". (only possible when SecOC_ VerifyStatusOverride is used)
	SECOC_VERIFICATIONFAILURE_ OVERWRITTEN	0x05	Verification failed, but the I-PDU was passed on to the upper layer due to the override status for this PDU. (only possible when SecOC_VerifyStatus Override is used)
Description	Enumeration to indicate verification results.		
Variation	--		
Available via	Rte_SecOC_Type.h		

](SRS_SecOC_00022)

8.8.5.3 SecOC_VerificationStatusType [SWS_SecOC_00160]⌈

Name	SecOC_VerificationStatusType	
Kind	Structure	
Elements	freshnessValueID	
	Type	uint16
	Comment	Identifier of the Freshness Value which resulted in the Verification Status
	verificationStatus	
	Type	SecOC_VerificationResultType
	Comment	Result of verification attempt: SECOC_VERIFICATIONSUCCESS = Verification successful SECOC_VERIFICATIONFAILURE = Verification not successful SECOC_FRESHNESSFAILURE = Verification not successful because of wrong freshness value SECOC_ AUTHENTICATIONBUILDFAILURE = Verification not successful because of wrong build authentication codes SECOC_NO_VERIFICATION = No verification attempt was performed on this I-PDU and the I-PDU was passed on to the upper layer "as is". SECOC_VERIFICATIONFAILURE_ OVERWRITTEN = Verification failed, but the I-PDU was passed on to the upper layer due to the override status for this PDU.
	secOCDataId	
	Type	uint16
	Comment	Data ID of SecOCDataId
Description	Data structure to bundle the status of a verification attempt for a specific Freshness Value and Data ID	
Variation	--	
Available via	Rte_SecOC_Type.h	

⌋(SRS_SecOC_00022)

8.8.5.4 SecOC_OverrideStatusType [SWS_SecOC_00991]⌈

Name	SecOC_OverrideStatusType		
Kind	Enumeration		
Range	SECOC_ OVERRIDE_ DROP_UNTIL_ NOTICE	0x00	Until further notice, authenticator verification is not performed (no CSM call) I-PDU is dropped, verification result is set to SECOC_NO_VERIFICATION.
	SECOC_ OVERRIDE_ DROP_UNTIL_	0x01	Until NumberOfMessagesToOverride is reached, authenticator verification is not performed (no CSM call) I-PDU is dropped, verification result is set to SECOC_NO_

	LIMIT		VERIFICATION.
	SECOC_ OVERRIDE_ CANCEL	0x02	Cancel Override of VerifyStatus.
	SECOC_ OVERRIDE_ PASS_UNTIL_ NOTICE	0x40	Until further notice, authenticator verification is performed, I-PDU is sent to upper layer independent of verification result, verification result is set to SECOC_ VERIFICATIONFAILURE_OVERWRITTEN in case of failed verification.
	SECOC_ OVERRIDE_ SKIP_UNTIL_ LIMIT	0x41	Until NumberOfMessagesToOverride is reached, authenticator verification is not performed, I-PDU is sent to upper layer, verification result is set to SECOC_NO_ VERIFICATION. If SecOCRxSecuredPduCollection is configured, SecOc shall process the SecOCRxAuthenticPdu without waiting for SecOCRxCryptographicPdu.
	SECOC_ OVERRIDE_ PASS_UNTIL_ LIMIT	0x42	Until NumberOfMessagesToOverride is reached, authenticator verification is performed, I-PDU is sent to upper layer independent of verification result, verification result is set to SECOC_VERIFICATIONFAILURE_ OVERWRITTEN in case of failed verification.
	SECOC_ OVERRIDE_ SKIP_UNTIL_ NOTICE	0x43	Until further notice, authenticator verification is not performed, I-PDU is sent to upper layer, verification result is set to SECOC_NO_VERIFICATION. If SecOCRxSecured PduCollection is configured, SecOc shall process the Sec OCRxAuthenticPdu without waiting for SecOCRx CryptographicPdu.
Description	Defines possibilities to override the verification status.		
Variation	--		
Available via	Rte_SecOC_Type.h		

](SRS_SecOC_00017)

9 Sequence diagrams

The sequence diagrams in the following sections show interactions between the SecOC module, the PduR and the upper layer and lower layer communication modules. These sequences serve as examples to express the different kinds of interactions that are served by the SecOC module for authentication and verification.

Note: The examples show the interaction with distinct bus interface (e.g FrIf), transport protocol module (e.g. CanTp) or upper layer communication module (e.g. COM) only. However, they are valid for other bus interfaces, transport protocol modules and upper layer communication modules as well.

9.1 Authentication of outgoing PDUs

9.1.1 Authentication during direct transmission

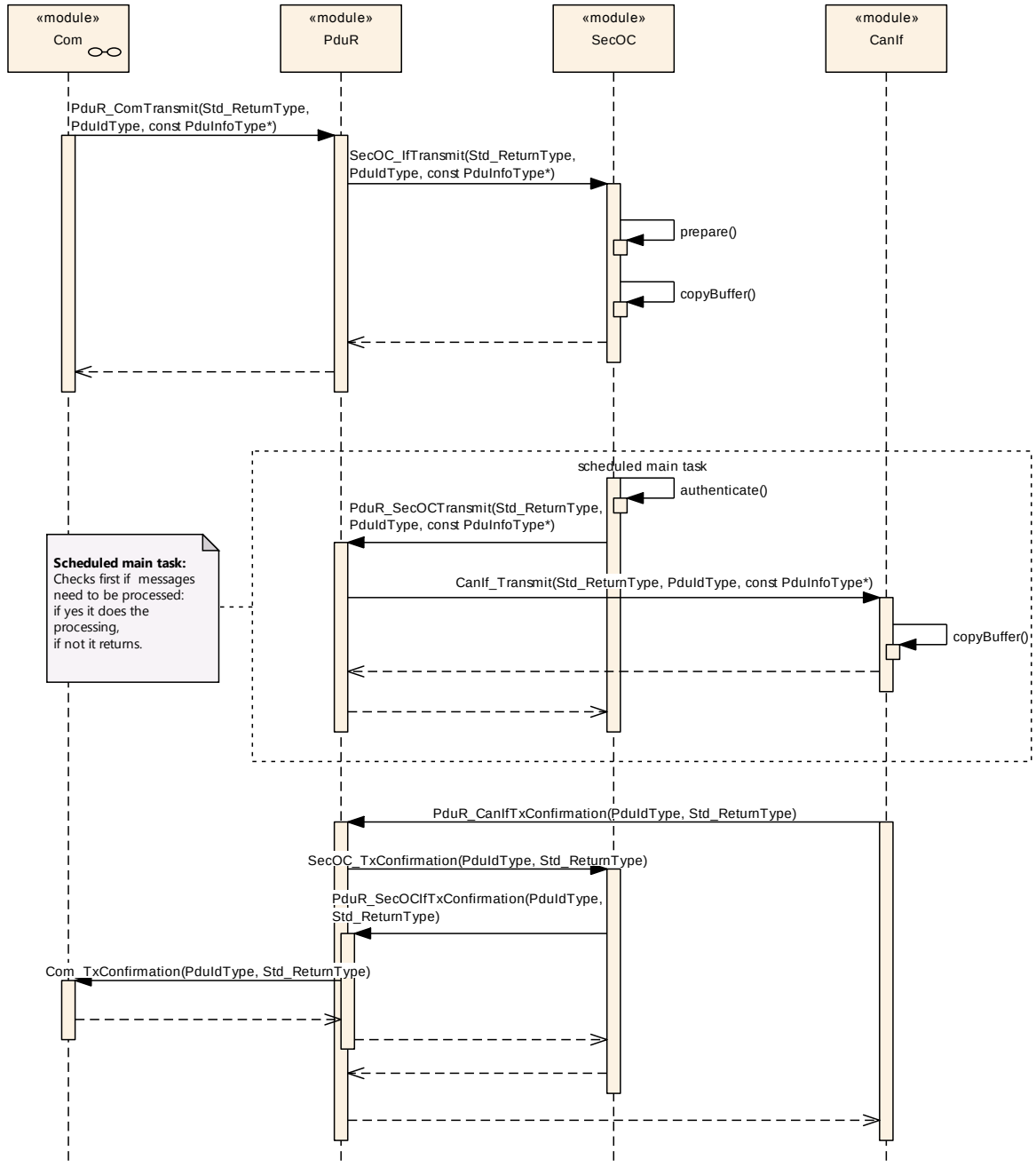

Figure 8: Authentication during direct transmission

9.1.2 Authentication during triggered transmission

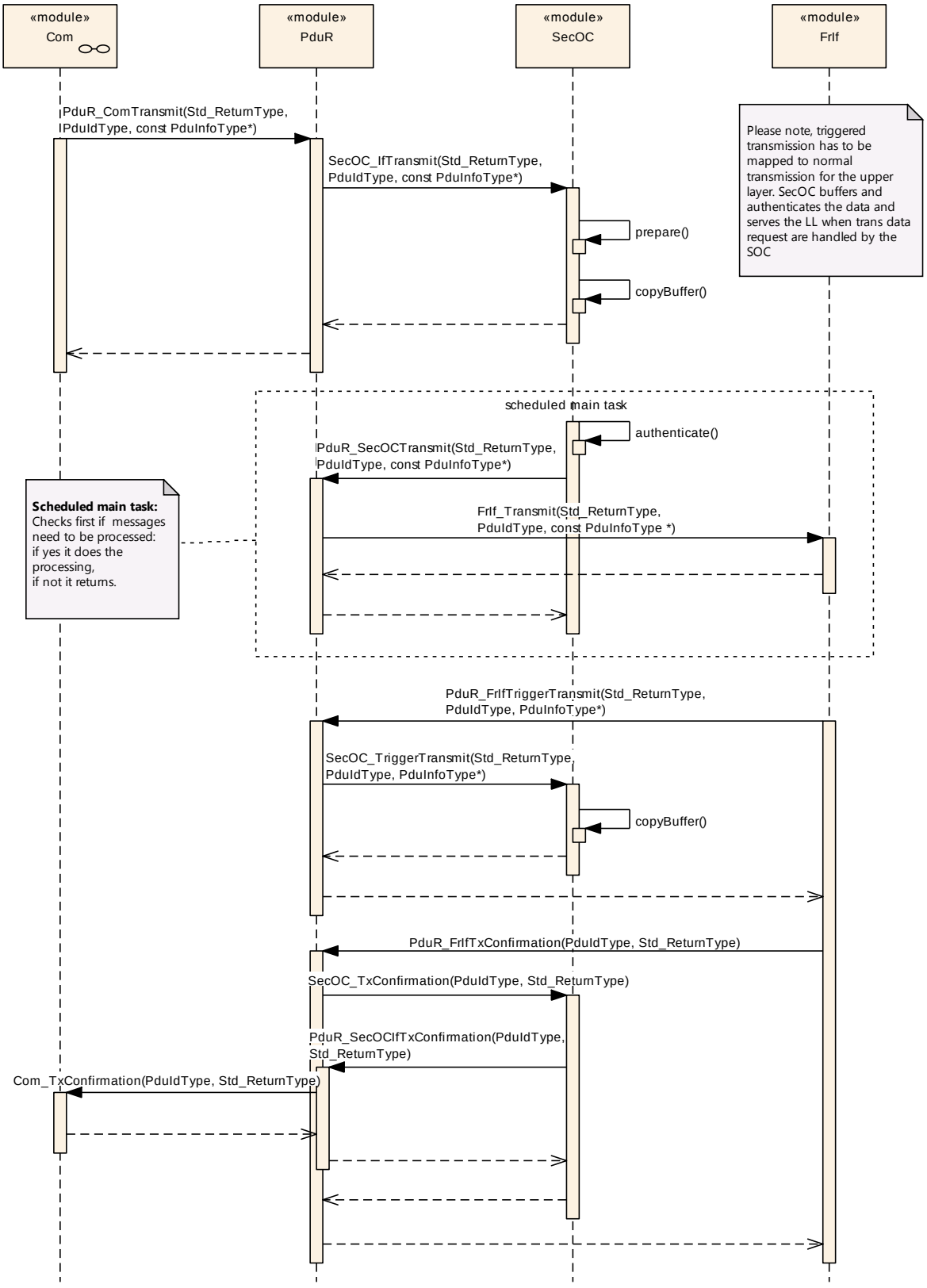

Figure 9: Authentication during Triggered Transmission

9.1.3 Authentication during transport protocol transmission

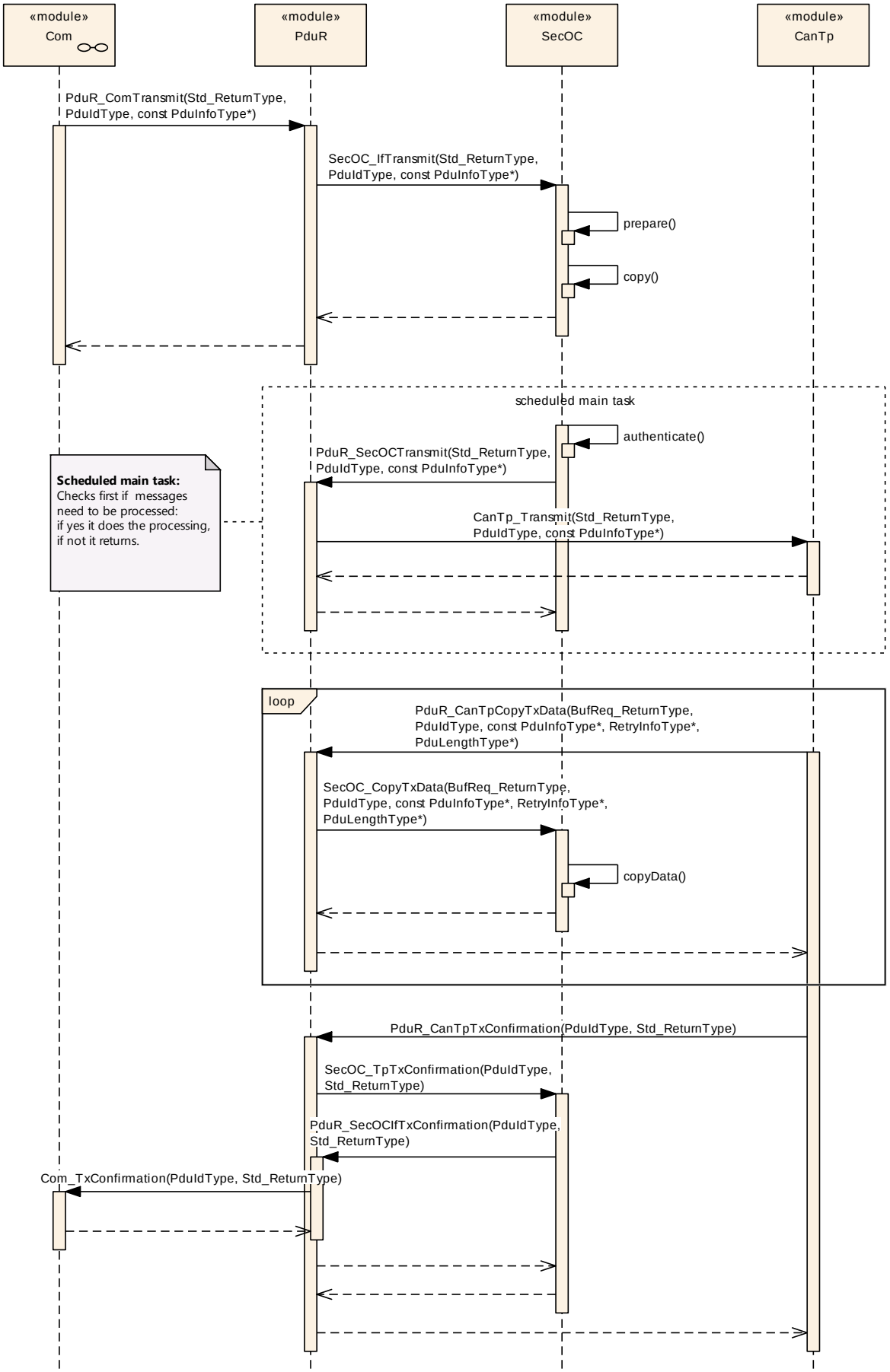
«module»
Com
«module»
PduR
«module»
SecOC
«module»
CanTp
PduR_ComTransmit(Std_ReturnType, PduIdType, const PduInfoType*)
SecOC_IfTransmit(Std_ReturnType, PduIdType, const PduInfoType*)
prepare()
copy()
scheduled main task
authenticate()
PduR_SecOCTransmit(Std_ReturnType, PduIdType, const PduInfoType*)
CanTp_Transmit(Std_ReturnType, PduIdType, const PduInfoType*)
Scheduled main task:
Checks first if messages need to be processed:
if yes it does the processing,
if not it returns.
loop
PduR_CanTpCopyTxData(BufReq_ReturnType, PduIdType, const PduInfoType*, RetryInfoType*, PduLengthType*)
SecOC_CopyTxData(BufReq_ReturnType, PduIdType, const PduInfoType*, RetryInfoType*, PduLengthType*)
copyData()
PduR_CanTpTxConfirmation(PduIdType, Std_ReturnType)
SecOC_TpTxConfirmation(PduIdType, Std_ReturnType)
PduR_SecOCIfTxConfirmation(PduIdType, Std_ReturnType)
Com_TxConfirmation(PduIdType, Std_ReturnType)

Figure 10:Authentication during TP transmission

9.1.4 Authentication with upper layer transport protocol

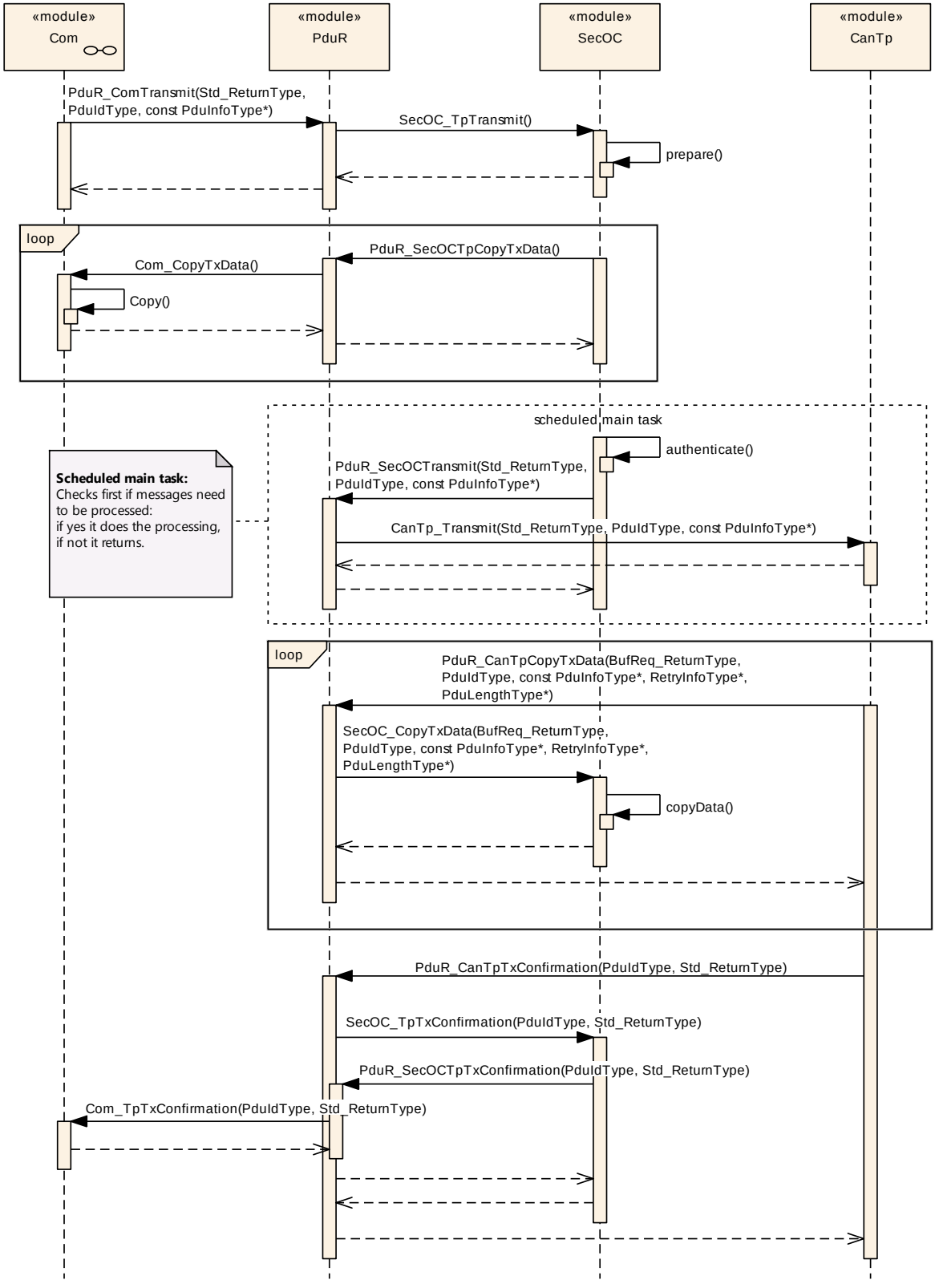

Figure 11: Authentication with upper layer TP

9.2 Verification of incoming PDUs

9.2.1 Verification during direct reception

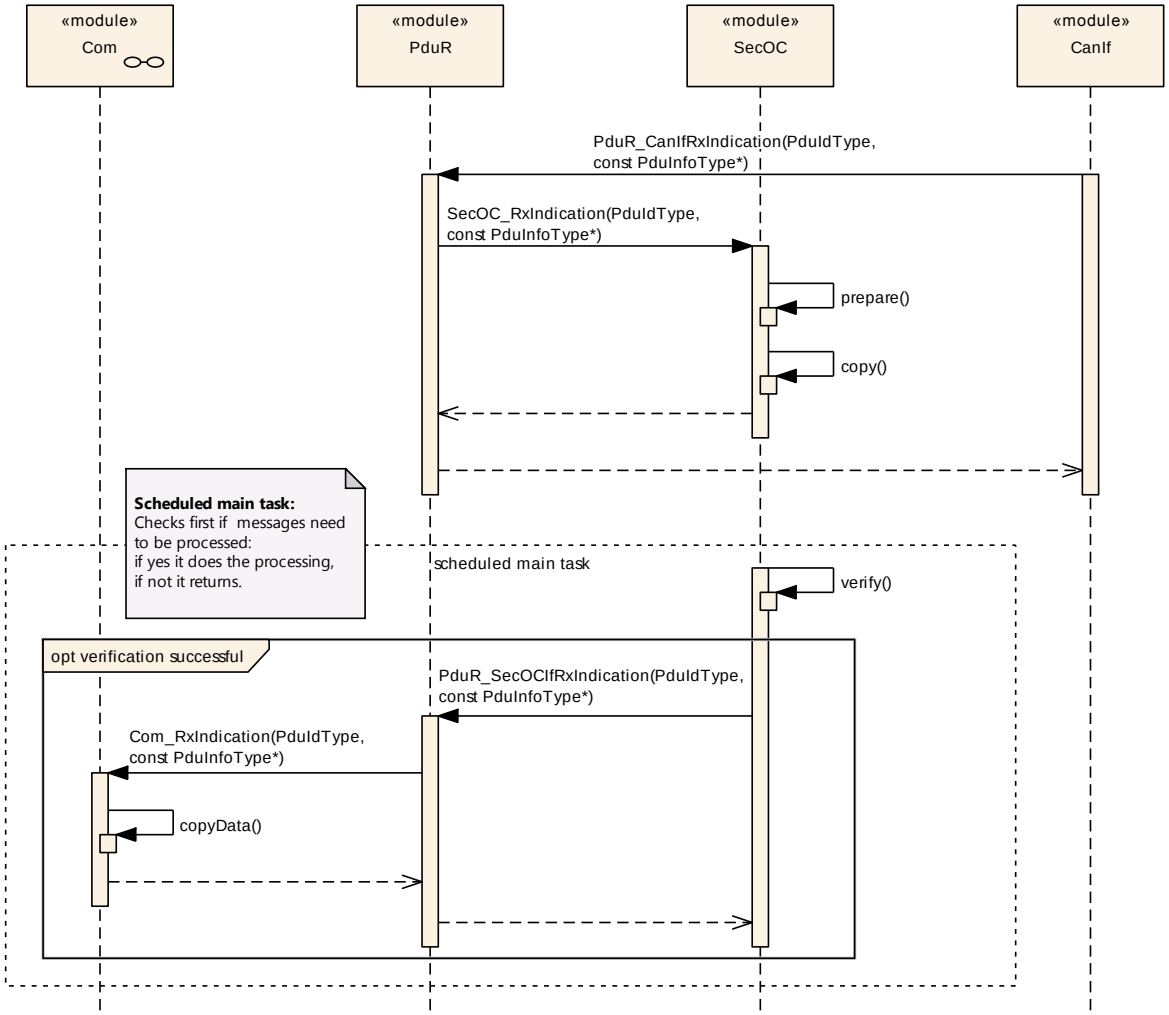

Figure 12: Verification during direct reception

9.2.2 Verification during transport protocol reception

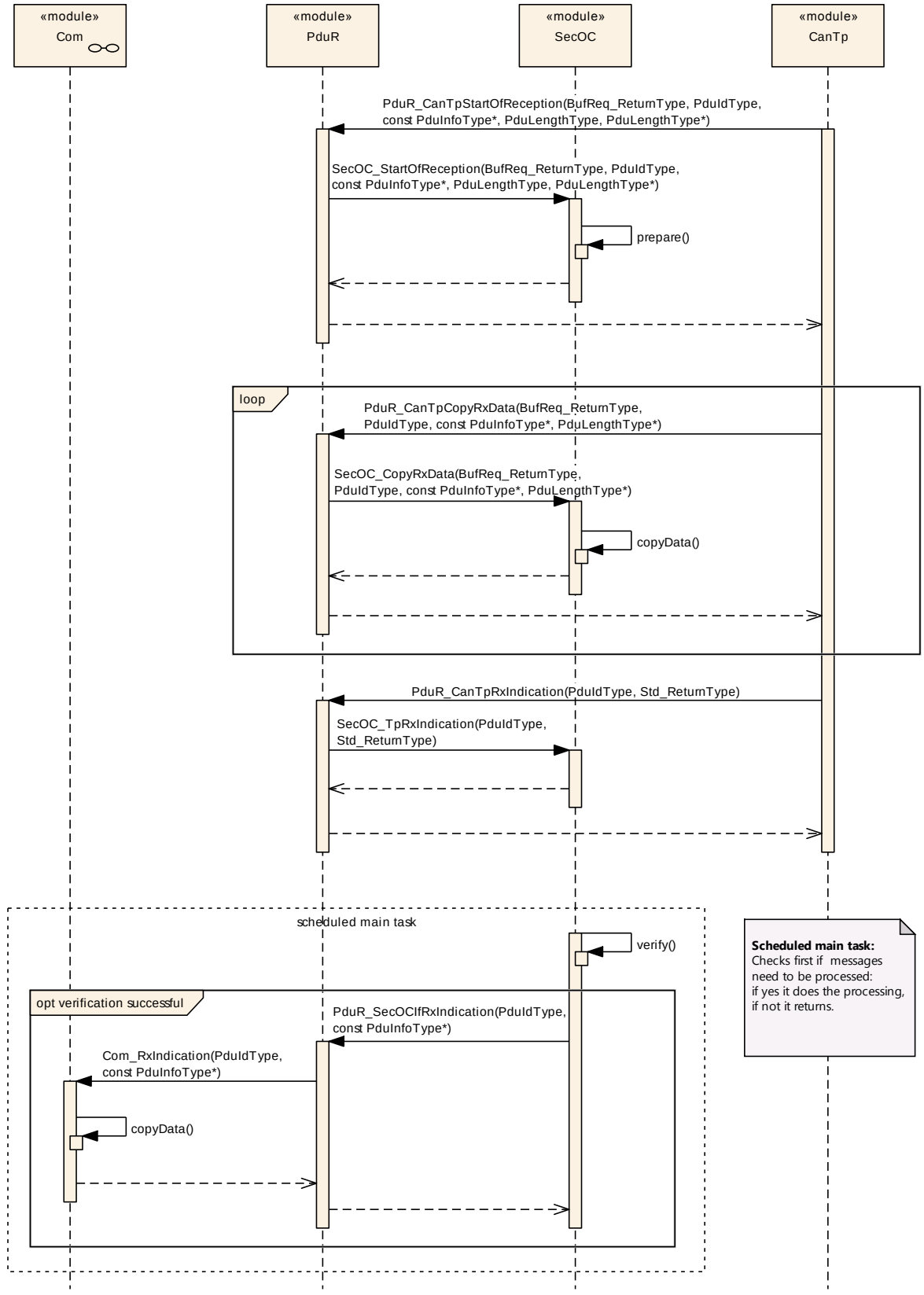

Figure 13: Verification during transport protocol reception

9.2.3 Verification with upper layer transport protocol

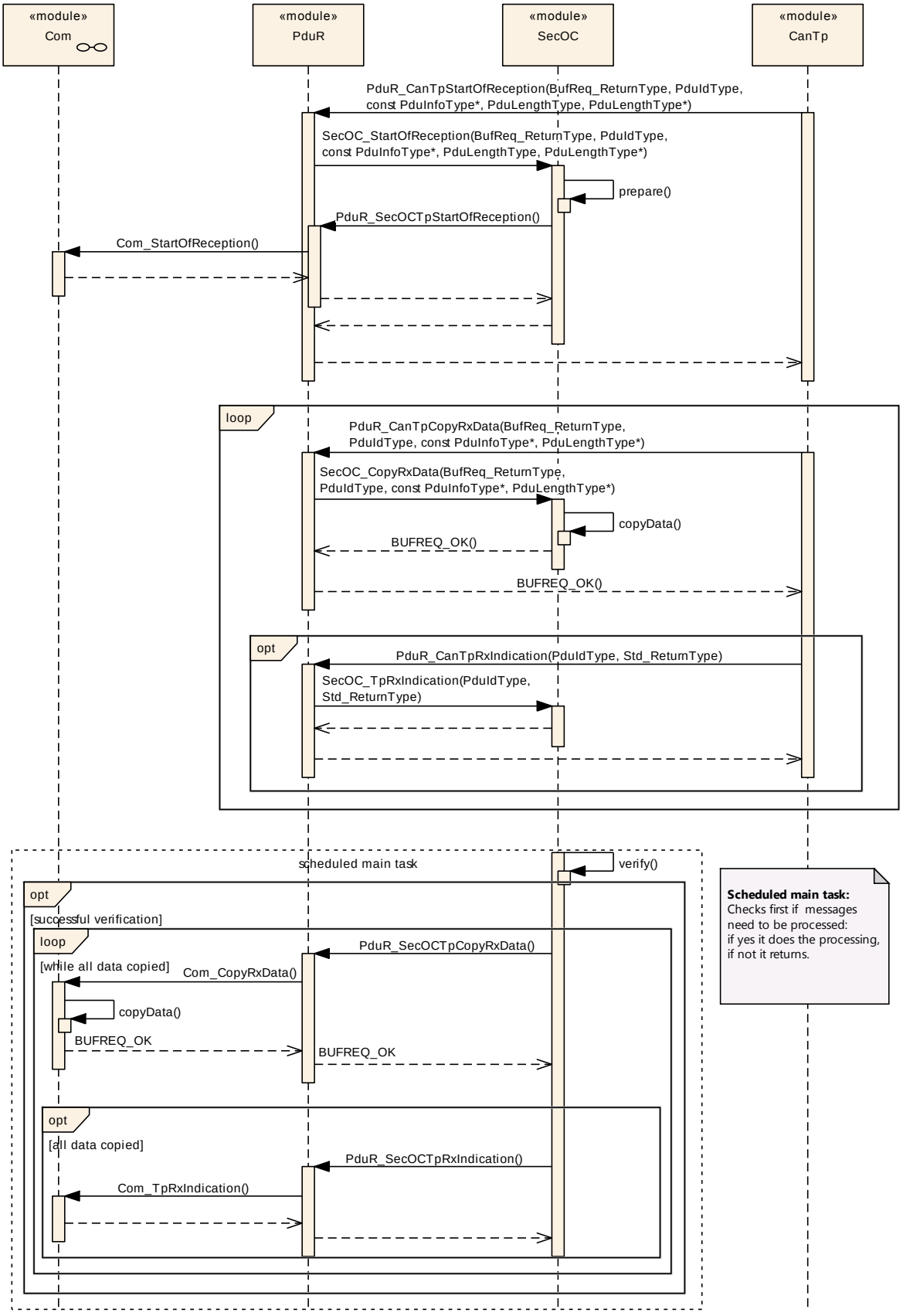

Figure 14: Verification with upper layer TP

9.3 Re-authentication Gateway

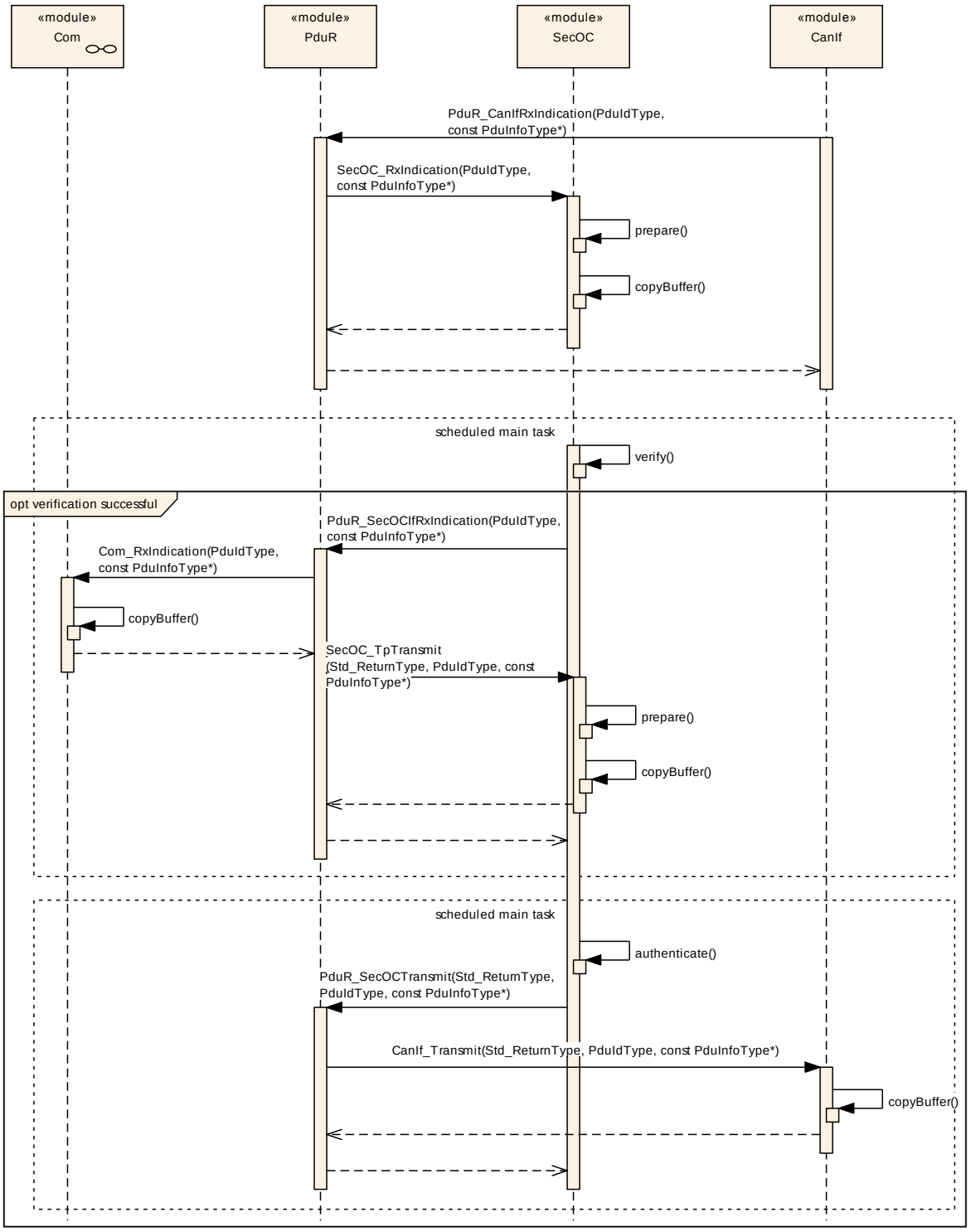

Figure 15: Verification and authentication in a gateway situation

9.4 Freshness Handling

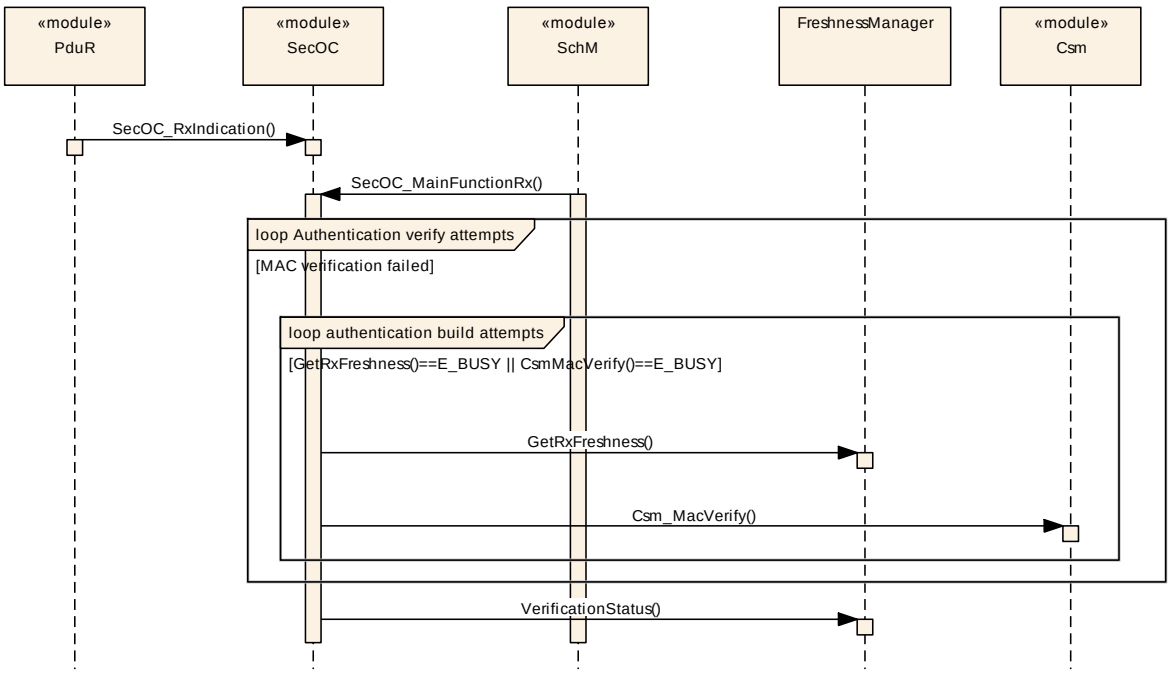

Figure 16:Freshness Handling

10 Configuration specification

The following chapters summarize all configuration parameters. The detailed meanings of the parameters are described in the Chaptersbelow.

10.1 Containers and configuration parameters

For an overview of the AUTOSAR SecOC module's configuration, see

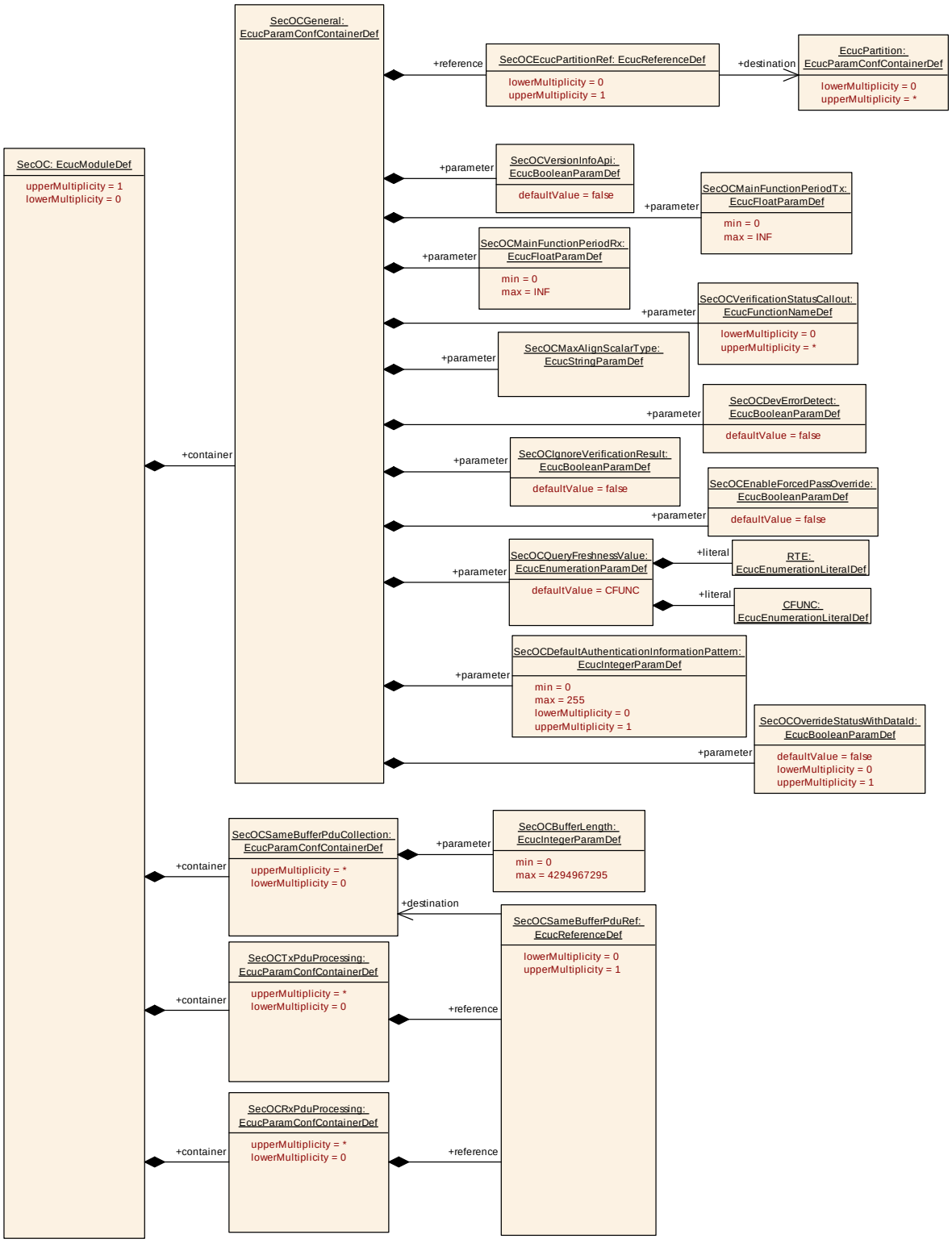

Figure 17: The AUTOSAR SecOC module's Configuration Overview

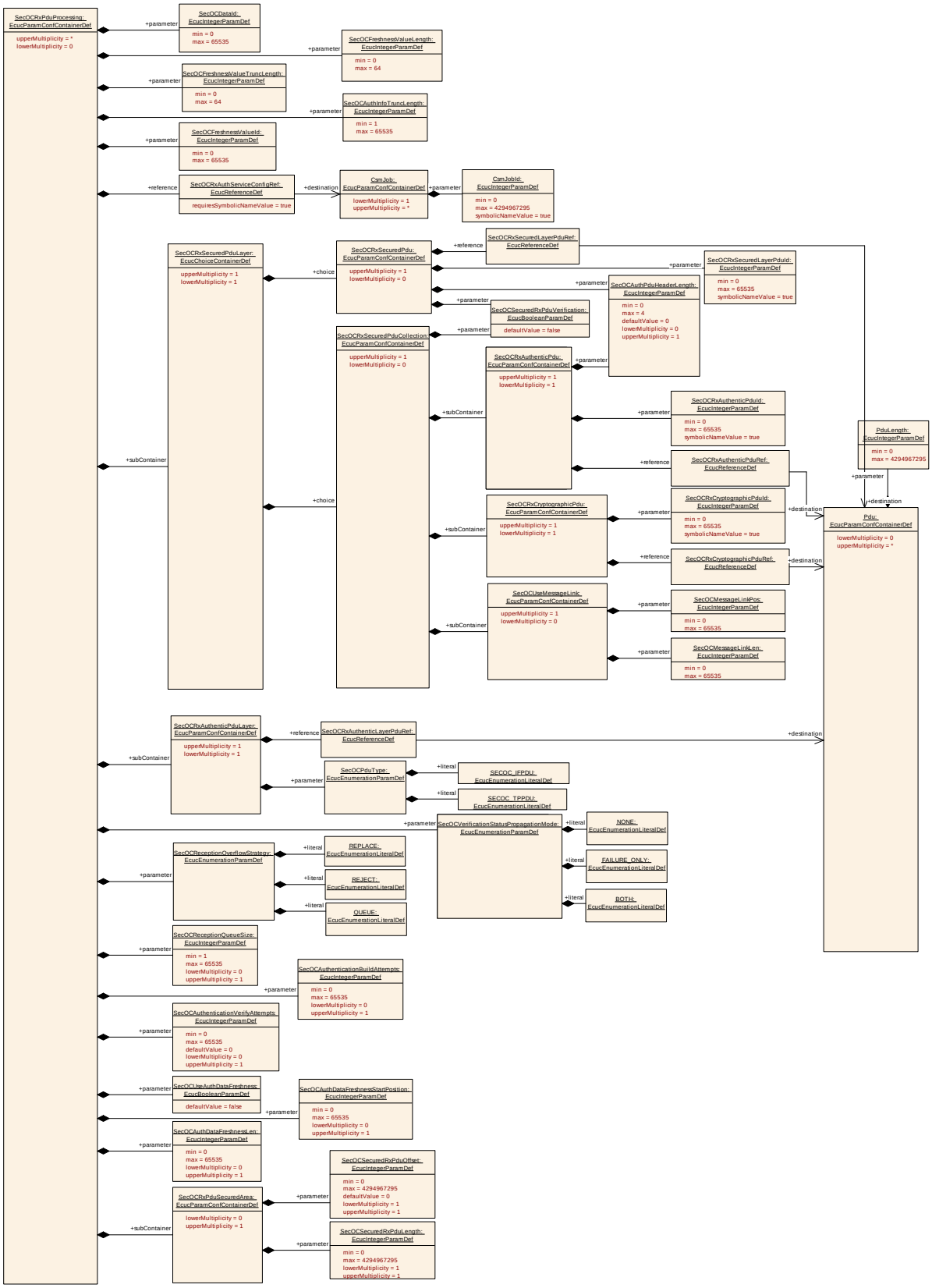

Figure 18: The AUTOSAR SecOC Rx Pdu Configuration

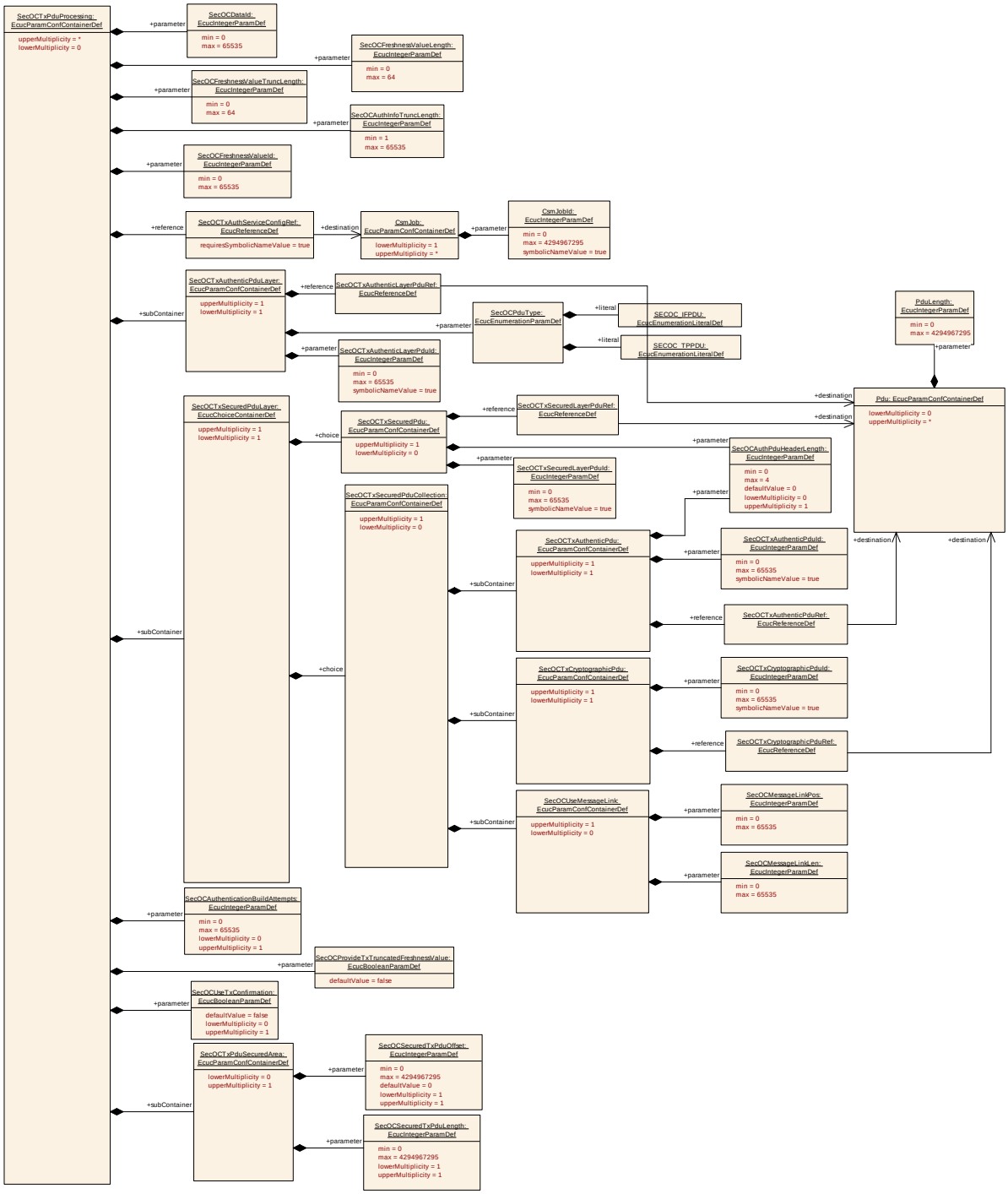

Figure 19: The AUTOSAR SecOC Tx Pdu Configuration

10.1.1 SecOC

SWS Item	**ECUC_SecOC_00001 :**
Module Name	*SecOC*
Module Description	Configuration of the SecOC (SecureOnboardCommunication) module.
Post-Build Variant Support	true
Supported Config Variants	VARIANT-LINK-TIME, VARIANT-POST-BUILD, VARIANT-PRE-COMPILE

Included Containers		
Container Name	***Multiplicity***	***Scope / Dependency***
SecOCGeneral	1	Contains the general configuration parameters of the SecOC module.
SecOCRxPduProcessing	0..*	Contains the parameters to configure the RxPdus to be verified by the SecOC module.
SecOCSameBufferPduCollection	0..*	SecOCBuffer configuration that may be used by a collection of Pdus.
SecOCTxPduProcessing	0..*	Contains the parameters to configure the TxPdus to be secured by the SecOC module.

10.1.2 SecOCGeneral

SWS Item	**ECUC_SecOC_00002 :**
Container Name	SecOCGeneral
Parent Container	SecOC
Description	Contains the general configuration parameters of the SecOC module.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00098 :**		
Name	SecOCDefaultAuthenticationInformationPattern		
Parent Container	SecOCGeneral		
Description	The parameter describes the behaviour of SecOC when authentication build counter has reached the configuration value SecOCAuthenticationBuildAttempts, or the query of the freshness function returns E_NOT_OK or the calculation of the authenticator has returned a non-recoverable error such as returning E_NOT_OK or KEY_FAILURE. If the configuration parameter is not present, SecOC module shall remove the Authentic I-PDU from its internal buffer and cancel the transmission request If the configuration parameter is present, SecOC will use this value for each byte of Freshness Value and Authenticator when building the Authentication Information, and will not cancel the transmission request.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 255		
Default value	--		
Post-Build Variant Multiplicity	false		
Post-Build Variant Value	false		
Multiplicity Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00007 :**		
Name	SecOCDevErrorDetect		
Parent Container	SecOCGeneral		
Description	Switches the development error detection and notification on or off. • true: detection and notification is enabled. • false: detection and notification is disabled.		
Multiplicity	1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00051 :**		
Name	SecOCEnableForcedPassOverride		
Parent Container	SecOCGeneral		
Description	When this configuration option is set to TRUE then the functionality inside the function SecOC_VerifyStatusOverride to send I-PDUs to upper layer independent of the verification result is enabled.		
Multiplicity	1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00052 :**		
Name	SecOCIgnoreVerificationResult		
Parent Container	SecOCGeneral		
Description	The result of the authentication process (e.g. MAC Verify) is ignored after the first try and the SecOC proceeds like the result was a success. The calculation of the authenticator is still done, only its result will be ignored. ▪ true: enabled (verification result is ignored). ▪ false: disabled (verification result is NOT ignored).		
Multiplicity	1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00053 :**		
Name	SecOCMainFunctionPeriodRx		
Parent Container	SecOCGeneral		
Description	Allows to configure the time for the MainFunction of the Rx path (as float in seconds).		
Multiplicity	1		
Type	EcucFloatParamDef		
Range	]0 .. INF[		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: ECU		

SWS Item	**ECUC_SecOC_00054 :**
Name	SecOCMainFunctionPeriodTx
Parent Container	SecOCGeneral
Description	Allows to configure the time for the MainFunction of the Tx path (as float in seconds).
Multiplicity	1

Type	EcucFloatParamDef		
Range	]0 .. INF[		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: ECU		

SWS Item	**ECUC_SecOC_00047 :**		
Name	SecOCMaxAlignScalarType		
Parent Container	SecOCGeneral		
Description	The scalar type which has the maximum alignment restrictions on the given platform. This type can be e.g. uint8, uint16 or uint32.		
Multiplicity	1		
Type	EcucStringParamDef		
Default value	--		
maxLength	--		
minLength	--		
regularExpression	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00099 :**		
Name	SecOCOverrideStatusWithDataId		
Parent Container	SecOCGeneral		
Description	This option defines if the parameter "ValueId" of the function SecOC_VerifyStatusOverride() accepts the freshness value (as a collection of one or more Secured I-PDUs to freshness) or the dataID for individual Secured I-PDUs. • true: Function SecOC_VerifyStatusOverride accepts SecOCDataId as parameter. • false: Function SecOC_VerifyStatusOverride accepts SecOCFreshnessValueId as parameter.		
Multiplicity	0..1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00078 :**	
Name	SecOCQueryFreshnessValue	
Parent Container	SecOCGeneral	
Description	This parameter specifies if the freshness value shall be determined through a C-function (CD) or a software component (SW-C).	
Multiplicity	1	
Type	EcucEnumerationParamDef	
Range	CFUNC	The SecOC queries the freshness for every

		PDU to process using C function API	
	RTE	The SecOC queries the freshness for every PDU to process using the Rte service port FreshnessManagement	
Default value	CFUNC		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency			

SWS Item	**ECUC_SecOC_00004 :**		
Name	SecOCVerificationStatusCallout		
Parent Container	SecOCGeneral		
Description	Entry address of the customer specific call out routine which shall be invoked in case of a verification attempt.		
Multiplicity	0..*		
Type	EcucFunctionNameDef		
Default value	--		
maxLength	--		
minLength	--		
regularExpression	--		
Post-Build Variant Multiplicity	false		
Post-Build Variant Value	false		
Multiplicity Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00003 :**		
Name	SecOCVersionInfoApi		
Parent Container	SecOCGeneral		
Description	If true the SecOC_GetVersionInfo API is available.		
Multiplicity	1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00100 :**
Name	SecOCEcucPartitionRef
Parent Container	SecOCGeneral
Description	Reference to EcucPartition, where SecOC module is assigned to. **Tags:** atp.Status=draft
Multiplicity	0..1
Type	Reference to [EcucPartition]

Post-Build Variant Multiplicity	false		
Post-Build Variant Value	false		
Multiplicity Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

No Included Containers

SWS Item	**ECUC_SecOC_00094 :**		
Name	SecOCOverrideStatusWithDataId		
Parent Container	SecOCGeneral		
Description	This option defines if the parameter "ValueId" of the function SecOC_VerifyStatusOverride() accepts the freshness value (as a collection of one or more Secured I-PDUs to freshness) or the dataID for individual Secured I-PDUs. • true: Function SecOC_VerifyStatusOverride accepts SecOCDataId as parameter. ▪ false: Function SecOC_VerifyStatusOverride accepts SecOCFreshnessValueId as parameter.		
Multiplicity	0..1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

10.1.3 SecOCSameBufferPduCollection

SWS Item	**ECUC_SecOC_00009 :**		
Container Name	SecOCSameBufferPduCollection		
Parent Container	SecOC		
Description	SecOCBuffer configuration that may be used by a collection of Pdus.		
Post-Build Variant Multiplicity	false		
Multiplicity Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Configuration Parameters			

SWS Item	**ECUC_SecOC_00008 :**
Name	SecOCBufferLength
Parent Container	SecOCSameBufferPduCollection
Description	This parameter defines the Buffer in bytes that is used by the SecOC

	module.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 4294967295		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

No Included Containers

10.1.4 SecOCRxPduProcessing

SWS Item	**ECUC_SecOC_00011 :**
Container Name	SecOCRxPduProcessing
Parent Container	SecOC
Description	Contains the parameters to configure the RxPdus to be verified by the SecOC module.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00082 :**		
Name	SecOCAuthDataFreshnessLen		
Parent Container	SecOCRxPduProcessing		
Description	The length of the external authentic PDU data in bits (uint16).		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: ECU		

SWS Item	**ECUC_SecOC_00081 :**		
Name	SecOCAuthDataFreshnessStartPosition		
Parent Container	SecOCRxPduProcessing		
Description	This value determines the start position in bits (uint16) of the Authentic PDU that shall be passed on to the Freshness SWC. The bit position starts counting from the MSB of the first byte of the PDU.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: ECU		

SWS Item	**ECUC_SecOC_00079 :**

Name	SecOCAuthenticationBuildAttempts		
Parent Container	SecOCRxPduProcessing		
Description	This parameter specifies the number of authentication build attempts.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00080 :**		
Name	SecOCAuthenticationVerifyAttempts		
Parent Container	SecOCRxPduProcessing		
Description	This parameter specifies the number of authentication verify attempts that are to be carried out when the verification of the authentication information failed for a given Secured I-PDU. If zero is set, then only one authentication verification attempt is done.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	0		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00095 :**		
Name	SecOCAuthInfoTruncLength		
Parent Container	SecOCRxPduProcessing		
Description	This parameter defines the length in bits of the authentication code to be included in the payload of the Secured I-PDU.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	1 .. 65535		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00030 :**		
Name	SecOCDataId		
Parent Container	SecOCRxPduProcessing		
Description	This parameter defines a unique numerical identifier for the Secured I-PDU.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE

	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00038 :**		
Name	SecOCFreshnessValueId		
Parent Container	SecOCRxPduProcessing		
Description	This parameter defines the Id of the Freshness Value. The Freshness Value might be a normal counter or a time value.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00031 :**		
Name	SecOCFreshnessValueLength		
Parent Container	SecOCRxPduProcessing		
Description	This parameter defines the complete length in bits of the Freshness Value. As long as the key doesn't change the counter shall not overflow. The length of the counter shall be determined based on the expected life time of the corresponding key and frequency of usage of the counter.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 64		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00094 :**		
Name	SecOCFreshnessValueTruncLength		
Parent Container	SecOCRxPduProcessing		
Description	This parameter defines the length in bits of the Freshness Value to be included in the payload of the Secured I-PDU. This length is specific to the least significant bits of the complete Freshness Counter. If the parameter is 0 no Freshness Value is included in the Secured I-PDU.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 64		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local dependency: SecOCFreshnessCounterTxLength ≤ SecOCFreshnessCounterLength		

SWS Item	**ECUC_SecOC_00076 :**

Name	SecOCReceptionOverflowStrategy		
Parent Container	SecOCRxPduProcessing		
Description	This parameter defines the overflow strategy for receiving PDUs		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	QUEUE	Subsequent received message will be queued	
	REJECT	Subsequent received message will be discarded	
	REPLACE	Subsequent received message will replace the currently processed message	
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00077 :**		
Name	SecOCReceptionQueueSize		
Parent Container	SecOCRxPduProcessing		
Description	This parameter defines the queue size in case the overflow strategy for receiving PDUs is set to QUEUE.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	1 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00083 :**		
Name	SecOCUseAuthDataFreshness		
Parent Container	SecOCRxPduProcessing		
Description	A Boolean value that indicates if a part of the Authentic-PDU shall be passed on to the SWC that verifies and generates the Freshness. If it is set to TRUE, the values SecOCAuthDataFreshnessStartPosition and SecOCAuthDataFreshnessLen must be set to specify the bit position and length within the Authentic-PDU.		
Multiplicity	1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: ECU		

SWS Item	**ECUC_SecOC_00046 :**
Name	SecOCVerificationStatusPropagationMode
Parent Container	SecOCRxPduProcessing
Description	This parameter is used to describe the propagation of the status of each verification

	attempt from the SecOC module to SWCs.		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	BOTH	Both "True" and "False" AuthenticationStatus is propagated to SWC	
	FAILURE_ONLY	Only "False" AuthenticationStatus is propagated to SWC	
	NONE	No AuthenticationStatus is propagated to SWC	
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00048 :**
Name	SecOCRxAuthServiceConfigRef
Parent Container	SecOCRxPduProcessing
Description	This reference is used to define which crypto service function is called for authentication. If PDUs with a dynamic length are used (e.g. CanTP or Dynamic Length PDUs) a MAC algorithm has to be chosen, that is not vulnerable to length extension attack (e.g. CMAC/HMAC).
Multiplicity	1
Type	Symbolic name reference to [CsmJob]
Post-Build Variant Value	false
Scope / Dependency	

SWS Item	**ECUC_SecOC_00049 :**		
Name	SecOCSameBufferPduRef		
Parent Container	SecOCRxPduProcessing		
Description	This reference is used to collect Pdus that are using the same SecOC buffer.		
Multiplicity	0..1		
Type	Reference to [SecOCSameBufferPduCollection]		
Post-Build Variant Multiplicity	false		
Post-Build Variant Value	false		
Multiplicity Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

Included Containers		
Container Name	***Multiplicity***	***Scope / Dependency***
SecOCRxAuthenticPduLayer	1	This container specifies the Pdu that is transmitted by the SecOC module to the PduR after the Mac was verified.
SecOCRxPduSecuredArea	0..1	This container specifies an area in the Authentic I-Pdu that will be the input to the Authenticator verification algorithm. If this container does not exist in the configuration the complete Authentic I-Pdu will be the input to the Authenticator

		verification algorithm.
SecOCRxSecuredPduLayer	1	This container specifies the Pdu that is received by the SecOC module from the PduR. For this Pdu the Mac verification is provided.

10.1.5 SecOCRxSecuredPduLayer

SWS Item	**ECUC_SecOC_00041 :**
Choice container Name	SecOCRxSecuredPduLayer
Parent Container	SecOCRxPduProcessing
Description	This container specifies the Pdu that is received by the SecOC module from the PduR. For this Pdu the Mac verification is provided.

Container Choices		
Container Name	***Multiplicity***	***Scope / Dependency***
SecOCRxSecuredPdu	0..1	This container specifies the Pdu that is received by the SecOC module from the PduR. For this Pdu the Mac verification is provided.
SecOCRxSecuredPduCollection	0..1	This container specifies two Pdus that are received by the SecOC module from the PduR and a message linking between them. SecOCRxAuthenticPdu contains the original Authentic I-PDU, i.e. the secured data, and the SecOCRxCryptographicPdu contains the Authenticator, i.e. the actual Authentication Information.

10.1.6 SecOCRxSecuredPdu

SWS Item	**ECUC_SecOC_00069 :**
Container Name	SecOCRxSecuredPdu
Parent Container	SecOCRxSecuredPduLayer
Description	This container specifies the Pdu that is received by the SecOC module from the PduR. For this Pdu the Mac verification is provided.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00093 :**		
Name	SecOCAuthPduHeaderLength		
Parent Container	SecOCRxSecuredPdu		
Description	This parameter indicates the length (in bytes) of the Secured I-PDU Header in the Secured I-PDU. The length of zero means there's no header in the PDU.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 4		
Default value	0		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00043 :**		
Name	SecOCRxSecuredLayerPduId		
Parent Container	SecOCRxSecuredPdu		
Description	PDU identifier assigned by SecOC module. Used by PduR for SecOC_[If|Tp]RxIndication.		
Multiplicity	1		
Type	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00092 :**		
Name	SecOCSecuredRxPduVerification		
Parent Container	SecOCRxSecuredPdu		
Description	This parameter defines whether the signature authentication or MAC verification shall be performed on this Secured I-PDU. If set to false, the SecOC module extracts the Authentic I-PDU from the Secured I-PDU without verification.		
Multiplicity	1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00042 :**		
Name	SecOCRxSecuredLayerPduRef		
Parent Container	SecOCRxSecuredPdu		
Description	Reference to the global Pdu.		
Multiplicity	1		
Type	Reference to [Pdu]		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.7 SecOCRxAuthenticPduLayer

SWS Item	**ECUC_SecOC_00044 :**
Container Name	SecOCRxAuthenticPduLayer
Parent Container	SecOCRxPduProcessing

Description	This container specifies the Pdu that is transmitted by the SecOC module to the PduR after the Mac was verified.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00075 :**		
Name	SecOCPduType		
Parent Container	SecOCRxAuthenticPduLayer		
Description	This parameter defines API Type to use for communication with PduR.		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	SECOC_IFPDU	SECOC_IFPDU Interface communication API	
	SECOC_TPPDU	SECOC_TPPDU Transport Protocol communication API	
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00045 :**		
Name	SecOCRxAuthenticLayerPduRef		
Parent Container	SecOCRxAuthenticPduLayer		
Description	Reference to the global Pdu.		
Multiplicity	1		
Type	Reference to [Pdu]		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.8 SecOCRxSecuredPduCollection

SWS Item	**ECUC_SecOC_00067 :**
Container Name	SecOCRxSecuredPduCollection
Parent Container	SecOCRxSecuredPduLayer
Description	This container specifies two Pdus that are received by the SecOC module from the PduR and a message linking between them. SecOCRxAuthenticPdu contains the original Authentic I-PDU, i.e. the secured data, and the SecOCRxCryptographicPdu contains the Authenticator, i.e. the actual Authentication Information.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00092 :**
Name	SecOCSecuredRxPduVerification
Parent Container	SecOCRxSecuredPduCollection
Description	This parameter defines whether the signature authentication or MAC

	verification shall be performed on this Secured I-PDU. If set to false, the SecOC module extracts the Authentic I-PDU from the Secured I-PDU without verification.		
Multiplicity	1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

Included Containers		
Container Name	***Multiplicity***	***Scope / Dependency***
SecOCRxAuthenticPdu	1	This container specifies the PDU (that is received by the SecOC module from the PduR) which contains the Secured I-PDU Header and the Authentic I-PDU.
SecOCRxCryptographicPdu	1	This container specifies the Cryptographic Pdu that is received by the SecOC module from the PduR.
SecOCUseMessageLink	0..1	SecOC links an Authentic I-PDU and Cryptographic I-PDU together by repeating a specific part (Message Linker) of the Authentic I-PDU in the Cryptographic I-PDU.

[SWS_SecOC_CONSTR_00265]⌈
Within the same configured `SecOCRxPduProcessing`, if `SecOCReceptionOverflowStrategy` is set to `QUEUE`, then `SecOCRxSecuredPduCollection` shall have multiplicity of 0.
⌋ ()

10.1.9 SecOCRxCryptographicPdu

SWS Item	**ECUC_SecOC_00064 :**
Container Name	SecOCRxCryptographicPdu
Parent Container	SecOCRxSecuredPduCollection
Description	This container specifies the Cryptographic Pdu that is received by the SecOC module from the PduR.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00065 :**		
Name	SecOCRxCryptographicPduId		
Parent Container	SecOCRxCryptographicPdu		
Description	PDU identifier of the Cryptographic I-PDU assigned by SecOC module. Used by PduR for SecOC_IfRxIndication.		
Multiplicity	1		
Type	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00066 :**		
Name	SecOCRxCryptographicPduRef		
Parent Container	SecOCRxCryptographicPdu		
Description	Reference to the global Pdu.		
Multiplicity	1		
Type	Reference to [Pdu]		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.10 SecOCRxAuthenticPdu

SWS Item	**ECUC_SecOC_00061 :**
Container Name	SecOCRxAuthenticPdu
Parent Container	SecOCRxSecuredPduCollection
Description	This container specifies the PDU (that is received by the SecOC module from the PduR) which contains the Secured I-PDU Header and the Authentic I-PDU.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00093 :**		
Name	SecOCAuthPduHeaderLength		
Parent Container	SecOCRxAuthenticPdu		
Description	This parameter indicates the length (in bytes) of the Secured I-PDU Header in the Secured I-PDU. The length of zero means there's no header in the PDU.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 4		
Default value	0		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00062 :**		
Name	SecOCRxAuthenticPduId		
Parent Container	SecOCRxAuthenticPdu		
Description	PDU identifier of the Authentic I-PDU assigned by SecOC module. Used by PduR for SecOC_IfRxIndication.		
Multiplicity	1		
Type	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	

Scope / Dependency	scope: local

SWS Item	**ECUC_SecOC_00063 :**		
Name	SecOCRxAuthenticPduRef		
Parent Container	SecOCRxAuthenticPdu		
Description	Reference to the global Pdu.		
Multiplicity	1		
Type	Reference to [Pdu]		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.11 SecOCTxPduProcessing

SWS Item	**ECUC_SecOC_00012 :**
Container Name	SecOCTxPduProcessing
Parent Container	SecOC
Description	Contains the parameters to configure the TxPdus to be secured by the SecOC module.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00079 :**		
Name	SecOCAuthenticationBuildAttempts		
Parent Container	SecOCTxPduProcessing		
Description	This parameter specifies the number of authentication build attempts.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00097 :**		
Name	SecOCAuthInfoTruncLength		
Parent Container	SecOCTxPduProcessing		
Description	This parameter defines the length in bits of the authentication code to be included in the payload of the Secured I-PDU.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	1 .. 65535		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME

	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00014 :**		
Name	SecOCDataId		
Parent Container	SecOCTxPduProcessing		
Description	This parameter defines a unique numerical identifier for the Secured I-PDU.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00021 :**		
Name	SecOCFreshnessValueId		
Parent Container	SecOCTxPduProcessing		
Description	This parameter defines the Id of the Freshness Value. The Freshness Value might be a normal counter or a time value.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00015 :**		
Name	SecOCFreshnessValueLength		
Parent Container	SecOCTxPduProcessing		
Description	This parameter defines the complete length in bits of the Freshness Value. As long as the key doesn't change the counter shall not overflow. The length of the counter shall be determined based on the expected life time of the corresponding key and frequency of usage of the counter.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 64		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00096 :**
Name	SecOCFreshnessValueTruncLength
Parent Container	SecOCTxPduProcessing
Description	This parameter defines the length in bits of the Freshness Value to be included in the payload of the Secured I-PDU. This length is specific to the least significant bits of the complete Freshness Counter. If the parameter is

	0 no Freshness Value is included in the Secured I-PDU.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 64		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local dependency: SecOCFreshnessCounterTxLength ≤ SecOCFreshnessCounterLength		

SWS Item	**ECUC_SecOC_00084 :**		
Name	SecOCProvideTxTruncatedFreshnessValue		
Parent Container	SecOCTxPduProcessing		
Description	This parameter specifies if the Tx query freshness function provides the truncated freshness info instead of generating this by SecOC In this case, SecOC shall add this data to the Authentic PDU instead of truncating the freshness value.		
Multiplicity	1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00085 :**		
Name	SecOCUseTxConfirmation		
Parent Container	SecOCTxPduProcessing		
Description	A Boolean value that indicates if the function SecOC_SPduTxConfirmation shall be called for this PDU.		
Multiplicity	0..1		
Type	EcucBooleanParamDef		
Default value	false		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00010 :**		
Name	SecOCSameBufferPduRef		
Parent Container	SecOCTxPduProcessing		
Description	This reference is used to collect Pdus that are using the same SecOC buffer.		
Multiplicity	0..1		
Type	Reference to [SecOCSameBufferPduCollection]		
Post-Build Variant Multiplicity	false		
Post-Build Variant Value	false		
Multiplicity Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	

Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00013 :**
Name	SecOCTxAuthServiceConfigRef
Parent Container	SecOCTxPduProcessing
Description	This reference is used to define which crypto service function is called for authentication. If PDUs with a dynamic length are used (e.g. CanTP or Dynamic Length PDUs) a MAC algorithm has to be chosen, that is not vulnerable to length extension attack (e.g. CMAC/HMAC).
Multiplicity	1
Type	Symbolic name reference to [CsmJob]
Post-Build Variant Value	false
Scope / Dependency	

Included Containers		
Container Name	***Multiplicity***	***Scope / Dependency***
SecOCTxAuthenticPduLayer	1	This container specifies the Pdu that is received by the SecOC module from the PduR. For this Pdu the Mac generation is provided.
SecOCTxPduSecuredArea	0..1	This container specifies an area in the Authentic I-Pdu that will be the input to the Authenticator generation algorithm. If this container does not exist in the configuration the complete Authentic I-Pdu will be the input to the Authenticator generation algorithm.
SecOCTxSecuredPduLayer	1	This container specifies the Pdu that is transmitted by the SecOC module to the PduR after the Mac was generated.

10.1.12 SecOCTxAuthenticPduLayer

SWS Item	**ECUC_SecOC_00023 :**
Container Name	SecOCTxAuthenticPduLayer
Parent Container	SecOCTxPduProcessing
Description	This container specifies the Pdu that is received by the SecOC module from the PduR. For this Pdu the Mac generation is provided.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00075 :**		
Name	SecOCPduType		
Parent Container	SecOCTxAuthenticPduLayer		
Description	This parameter defines API Type to use for communication with PduR.		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	SECOC_IFPDU	SECOC_IFPDU Interface communication API	
	SECOC_TPPDU	SECOC_TPPDU Transport Protocol communication API	
Post-Build Variant Value	false		
Value	***Pre-compile time***	X	All Variants

Configuration Class	***Link time***	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00026 :**		
Name	SecOCTxAuthenticLayerPduId		
Parent Container	SecOCTxAuthenticPduLayer		
Description	PDU identifier assigned by SecOC module. Used by PduR for SecOC_[If|Tp]Transmit.		
Multiplicity	1		
Type	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00025 :**		
Name	SecOCTxAuthenticLayerPduRef		
Parent Container	SecOCTxAuthenticPduLayer		
Description	Reference to the global Pdu.		
Multiplicity	1		
Type	Reference to [Pdu]		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.13 SecOCTxSecuredPduLayer

SWS Item	**ECUC_SecOC_00024 :**
Choice container Name	SecOCTxSecuredPduLayer
Parent Container	SecOCTxPduProcessing
Description	This container specifies the Pdu that is transmitted by the SecOC module to the PduR after the Mac was generated.

Container Choices		
Container Name	***Multiplicity***	***Scope / Dependency***
SecOCTxSecuredPdu	0..1	This container specifies one Pdu that is transmitted by the SecOC module to the PduR after the Mac was generated. This Pdu contains the cryptographic information.
SecOCTxSecuredPduCollection	0..1	This container specifies the Pdu that is transmitted by the SecOC module to the PduR after the Mac was generated. Two separate Pdus are transmitted to the PduR: Authentic I-PDU and Cryptographic I-PDU.

10.1.14 SecOCTxSecuredPdu

SWS Item	**ECUC_SecOC_00070 :**		
Container Name	SecOCTxSecuredPdu		
Parent Container	SecOCTxSecuredPduLayer		
Description	This container specifies one Pdu that is transmitted by the SecOC module to the PduR after the Mac was generated. This Pdu contains the cryptographic information.		
Configuration Parameters			

SWS Item	**ECUC_SecOC_00093 :**		
Name	SecOCAuthPduHeaderLength		
Parent Container	SecOCTxSecuredPdu		
Description	This parameter indicates the length (in bytes) of the Secured I-PDU Header in the Secured I-PDU. The length of zero means there's no header in the PDU.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 4		
Default value	0		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00028 :**		
Name	SecOCTxSecuredLayerPduId		
Parent Container	SecOCTxSecuredPdu		
Description	PDU identifier assigned by SecOC module. Used by PduR for confirmation (SecOC_[If|Tp]TxConfirmation) and for TriggerTransmit.		
Multiplicity	1		
Type	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00027 :**		
Name	SecOCTxSecuredLayerPduRef		
Parent Container	SecOCTxSecuredPdu		
Description	Reference to the global Pdu.		
Multiplicity	1		
Type	Reference to [Pdu]		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.15 SecOCTxSecuredPduCollection

SWS Item	**ECUC_SecOC_00071 :**
Container Name	SecOCTxSecuredPduCollection
Parent Container	SecOCTxSecuredPduLayer
Description	This container specifies the Pdu that is transmitted by the SecOC module to the PduR after the Mac was generated. Two separate Pdus are transmitted to the PduR: Authentic I-PDU and Cryptographic I-PDU.
Configuration Parameters	

Included Containers		
Container Name	***Multiplicity***	***Scope / Dependency***
SecOCTxAuthenticPdu	1	This container specifies the PDU (that is transmitted by the SecOC module to the PduR) which contains the Secured I-PDU Header and the Authentic I-PDU.
SecOCTxCryptographicPdu	1	This container specifies the Cryptographic Pdu that is transmitted by the SecOC module to the PduR after the Mac was generated.
SecOCUseMessageLink	0..1	SecOC links an Authentic I-PDU and Cryptographic I-PDU together by repeating a specific part (Message Linker) of the Authentic I-PDU in the Cryptographic I-PDU.

10.1.16 SecOCTxAuthenticPdu

SWS Item	**ECUC_SecOC_00072 :**
Container Name	SecOCTxAuthenticPdu
Parent Container	SecOCTxSecuredPduCollection
Description	This container specifies the PDU (that is transmitted by the SecOC module to the PduR) which contains the Secured I-PDU Header and the Authentic I-PDU.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00093 :**		
Name	SecOCAuthPduHeaderLength		
Parent Container	SecOCTxAuthenticPdu		
Description	This parameter indicates the length (in bytes) of the Secured I-PDU Header in the Secured I-PDU. The length of zero means there's no header in the PDU.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	0 .. 4		
Default value	0		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00055 :**

Name	SecOCTxAuthenticPduId		
Parent Container	SecOCTxAuthenticPdu		
Description	PDU identifier of the Authentic I-PDU assigned by SecOC module. Used by PduR for confirmation (SecOC_IfTxConfirmation) and for TriggerTransmit.		
Multiplicity	1		
Type	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00056 :**		
Name	SecOCTxAuthenticPduRef		
Parent Container	SecOCTxAuthenticPdu		
Description	Reference to the global Pdu.		
Multiplicity	1		
Type	Reference to [Pdu]		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.17 SecOCTxCryptographicPdu

SWS Item	**ECUC_SecOC_00073 :**
Container Name	SecOCTxCryptographicPdu
Parent Container	SecOCTxSecuredPduCollection
Description	This container specifies the Cryptographic Pdu that is transmitted by the SecOC module to the PduR after the Mac was generated.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00057 :**		
Name	SecOCTxCryptographicPduId		
Parent Container	SecOCTxCryptographicPdu		
Description	PDU identifier of the Cryptographic I-PDU assigned by SecOC module. Used by PduR for confirmation (SecOC_IfTxConfirmation) and for TriggerTransmit.		
Multiplicity	1		
Type	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00058 :**		
Name	SecOCTxCryptographicPduRef		
Parent Container	SecOCTxCryptographicPdu		
Description	Reference to the global Pdu.		
Multiplicity	1		
Type	Reference to [Pdu]		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.18 SecOCUseMessageLink

SWS Item	**ECUC_SecOC_00074 :**
Container Name	SecOCUseMessageLink
Parent Container	SecOCRxSecuredPduCollection, SecOCTxSecuredPduCollection
Description	SecOC links an Authentic I-PDU and Cryptographic I-PDU together by repeating a specific part (Message Linker) of the Authentic I-PDU in the Cryptographic I-PDU.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00060 :**		
Name	SecOCMessageLinkLen		
Parent Container	SecOCUseMessageLink		
Description	Length of the Message Linker inside the Authentic I-PDU in bits.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00059 :**		
Name	SecOCMessageLinkPos		
Parent Container	SecOCUseMessageLink		
Description	The position of the Message Linker inside the Authentic I-PDU in bits.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 65535		
Default value	--		
Post-Build Variant Value	false		
Value Configuration Class	***Pre-compile time***	X	All Variants
	Link time	--	
	Post-build time	--	
Scope / Dependency	scope: local		

No Included Containers

10.1.19 SecOCTxPduSecuredArea

SWS Item	**ECUC_SecOC_00086 :**
Container Name	SecOCTxPduSecuredArea
Parent Container	SecOCTxPduProcessing
Description	This container specifies an area in the Authentic I-Pdu that will be the input to the Authenticator generation algorithm. If this container does not exist in the configuration the complete Authentic I-Pdu will be the input to the Authenticator generation algorithm.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00088 :**		
Name	SecOCSecuredTxPduLength		
Parent Container	SecOCTxPduSecuredArea		
Description	This parameter defines the length (in bytes) of the area within the Pdu which shall be secured		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 4294967295		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	*Pre-compile time*	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00087 :**		
Name	SecOCSecuredTxPduOffset		
Parent Container	SecOCTxPduSecuredArea		
Description	This parameter defines the start position (offset in bytes) of the area within the Pdu which shall be secured		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 4294967295		
Default value	0		
Post-Build Variant Value	true		
Value Configuration Class	*Pre-compile time*	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.1.20 SecOCRxPduSecuredArea

SWS Item	**ECUC_SecOC_00089 :**
Container Name	SecOCRxPduSecuredArea

Parent Container	SecOCRxPduProcessing
Description	This container specifies an area in the Authentic I-Pdu that will be the input to the Authenticator verification algorithm. If this container does not exist in the configuration the complete Authentic I-Pdu will be the input to the Authenticator verification algorithm.
Configuration Parameters	

SWS Item	**ECUC_SecOC_00091 :**		
Name	SecOCSecuredRxPduLength		
Parent Container	SecOCRxPduSecuredArea		
Description	This parameter defines the length (in bytes) of the area within the Pdu which is secured		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 4294967295		
Default value	--		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

SWS Item	**ECUC_SecOC_00090 :**		
Name	SecOCSecuredRxPduOffset		
Parent Container	SecOCRxPduSecuredArea		
Description	This parameter defines the start position (offset in bytes) of the area within the Pdu which is secured		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	0 .. 4294967295		
Default value	0		
Post-Build Variant Value	true		
Value Configuration Class	***Pre-compile time***	X	VARIANT-PRE-COMPILE
	Link time	X	VARIANT-LINK-TIME
	Post-build time	X	VARIANT-POST-BUILD
Scope / Dependency	scope: local		

No Included Containers

10.2 Published Information

For details, refer to the chapter 10.3 “Published Information” in SWS_BSWGeneral.

11 Annex A: Application hints for the development of SW-C Freshness Value Manager

11.1 Overview of freshness value construction

The freshness value is provided to SecOC either by a SW-C or CD. SecOC specification provides the required interfaces to request the freshness value either for transmission or for reception of a Secured I-PDU and the required interfaces to propagate the information of a failed or successful transmission or reception. There are several ways to construct and synchronize freshness value across ECUs.

This chapter specifies three use cases (UC_SecOC_00200, UC_SecOC_00201, UC_SecOC_00202) that describe different ways how a freshness value shall be constructed.

11.2 Freshness Value Based on Single Freshness Counter

[UC_SecOC_00200]⌈
The Software Component Freshness Value Manager (FVM) shall provide the Freshness Value (FV) to SecOC.

The FV construction is based on Freshness Counters realized by means of individual message counters.⌋ ()

The FVM shall provide a Freshness Counter for each configured Freshness Value ID (parameter SecOCFreshnessValueId and SecOCSecondaryFreshnessValueId).

Construction
When using a Freshness Counter instead of a Timestamp, the Freshness Counter is incremented prior to providing the authentication information to SecOC on the receiver side.

To properly ensure freshness, the Freshness Counter on both sides of the communication channel should be incremented synchronically.

The Freshness Counter has to be incremented for each outgoing message that is intended to be recognized as an individual incoming message on the receiver side. On the receiver side, the MAC verification of each received message including the counter update shall be performed exactly once.

The FVM shall increment the Freshness Counter corresponding to SecOCFreshnessValueID by 1 (CNT ++) only if SecOC has started the transmission of the Secured I-PDU by calling the PduR for further routing.
If the transmission of the Secured I-PDU has been cancelled before, FVM should not increment the Freshness Counter corresponding to SecOCFreshnessValueID.

Please note that when Freshness Counters are used as a FV, the FVM may allow the usage of second Freshness Values.

Verification of I-PDUs

The FVM module shall construct Freshness Verify Value (i.e. the Freshness Value to be used for Verification) and provide it to SecOC. In the event the complete Freshness Value is transmitted in the secured I-PDU, it needs to be verified that the constructed FreshnessVerifyValue is larger than the last stored notion of the Freshness Value. If it is not larger than the last stored notion of the Freshness Value, the FVM shall stop the verification and drop the Secured I-PDU.
Otherwise, constructing the Authentication Verify Counter is defined as outlined by the following pseudo code.

```
If (SecOCFreshnessValueTruncLength = FreshnessValueLength)
{
  FreshnessVerifyValue = FreshnessValue parsed from Secured I-PDU;
}
Else
{
  If (FreshnessValue parsed from Secured I-PDU > least significant bits of
      FreshnessValue corresponding to SecOCFreshnessValueID)
  {
    Attempts = 0;
    FreshnessVerifyValue = most significant bits of FreshnessValue corresponding to
    SecOCFreshnessValueID | FreshnessValue parsed from Secured I-PDU;
  }
  Else
  {
    Attempts = 0;
    FreshnessVerifyValue = most significant bits of FreshnessValue corresponding to
    SecOCFreshnessValueID + 1 | FreshnessValue parsed from payload;
  }
}
```

11.3 Freshness Value Based on Single Freshness Timestamp

[UC_SecOC_00201]⌈
The Software Component Freshness Value Manager (FVM) shall provide the Freshness Value (FV) to SecOC.
The FV construction is based on Freshness Counters realized by means of Timestamps. ⌋ ()

Source of global time values

The global synchronized time can be used as base for the Freshness Timestamp,. This global synchronized time will have the same value at the sender and all receivers. Therefore its value can be used as Freshness Value with the advantage that it does not necessarily need to be transmitted within the Secured PDU itself and it does not need to be transmitted for every sender and receiver individually.

Resolution and precision of global time values
The FVM has to consider the resolution and precision of the used global time values.

Please note that when Freshness Timestamps are used as a FV, the FVM may allow the usage of an Acceptance Window mechanism.

Verification of I-PDUs
The SecOC module shall construct Freshness Verify Value (i.e. the Freshness Value to be used for Verification) and provide it to SecOC. In case of complete Freshness Value transmission, it needs to be verified that the constructed FreshnessVerifyValue is within the acceptance window defined by SecOCRxAcceptanceWindow. If it is not in that window, the SecOC module shall stop the verification and drop the Secured I-PDU.
Otherwise, constructing the Authentication Verify Value is defined as outlined by the following pseudo code.

```
If (SecOCFreshnessValueTruncLength = FreshnessValueLength)
{
  FreshnessVerifyValue = FreshnessValue parsed from Secured I-PDU;
}
Else
{
  If ((most significant bits of FreshnessValue corresponding to SecOCFreshnessValueID |
       FreshnessValue parsed from Secured I-PDU) < (max(0: (most significant bits of
       FreshnessValue corresponding to SecOCFreshnessValueID | least significant bits of
       FreshnessValue corresponding to SecOCFreshnessValueID) – SecOCRxAcceptanceWindow)))
  {
    Attempts = 0;
    FreshnessVerifyBaseValue = most significant bits of FreshnessValue corresponding to
    SecOCFreshnessValueID + 1;
  }
  Else
  {
    Attempts = 0;
    FreshnessVerifyBaseValue = most significant bits of FreshnessValue corresponding to
    SecOCFreshnessValueID;
  }
  FreshnessVerifyValue = FreshnessVerifyUpperValue = FreshnessVerifyLowerValue =
  FreshnessVerifyBaseValue | FreshnessValue parsed from Secured I-PDU;
}
```

11.4 Freshness Value Based on Multiple Freshness Counters

[UC_SecOC_00202] ⌈
Construction of Freshness value from decoupled counters.
The Freshness Value Manager (FVM) (SW-C or CDD) provide the Freshness Value (FV) to SecOC. FVM supports a master-slave synchronization mechanism for FV.
⌋ ()

The figure below shows the relationship between FV management master ECU and slave (Sender / Receiver) ECU.

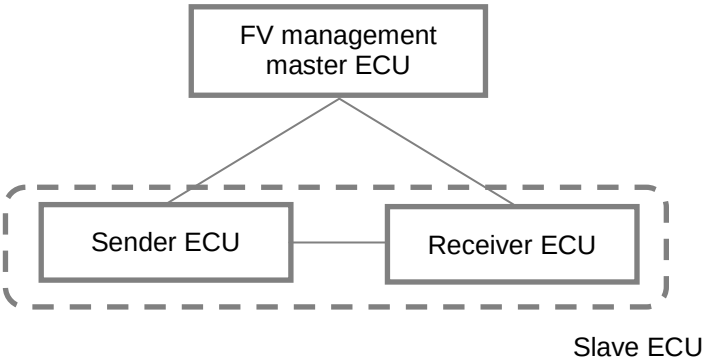

Figure 19: FvMaster Relationship Sender/Receiver ECU

Entity	*Description*
Sender ECU (Sender)	Sends a Secured I-PDU to the receiver ECU. Receives the synchronization message (TripResetSyncMsg) from the FV management master ECU and constructs the freshness value required to send the Secured I-PDU.
Receiver ECU (Receiver)	Receives a Secured I-PDU. Receives the synchronization message (TripResetSyncMsg) from the FV management master ECU and constructs the freshness value required to verify the received Secured I-PDU.
FV management master ECU (FvMaster)	Sends the synchronization message (TripResetSyncMsg) to all of the sender and receiver ECUs.

Table 1 - FvMaster Relationship Sender/Receiver ECU

FVM shall have a master synchronization function and a slave-transmission synchronization function. This will make it possible to implement the following two FV management master methods.

1. Single FV management master method
In this configuration, the system has only one FV management master ECU. For the system configuration and the entity list, see Figure 19 and Table 1, respectively.

2. Multi FV management master method
In this configuration, the system has multiple FV management master ECUs for the same number of sender ECUs. It means that a Sender ECU doubles as the FV management master entity ECU for secured I-PDUs which the Sender ECU manages. The system configuration and the entity list of the multi FV management master method are as follows.

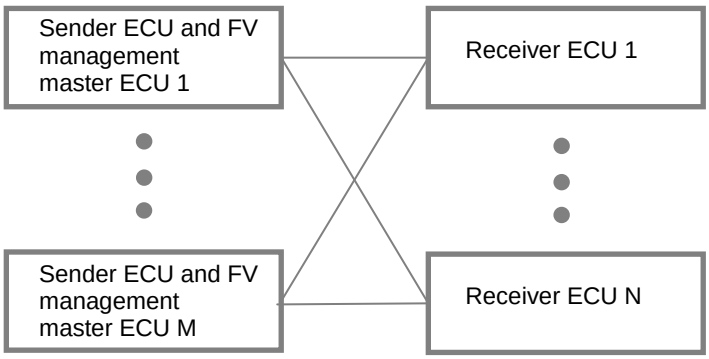

Figure 20: System Configuration for Multi FV Manager Master Method

Entity	Description
Sender ECU and FV management master ECU (Sender&FvMaster)	Sends a Secured I-PDU to the receiver ECU. Sends the synchronization message (TripResetSyncMsg) to the receiver ECU.
Receiver ECU (Receiver)	Receives a Secured I-PDU. Receives the synchronization message(TripResetSyncMsg).

Table 2 - Entity List for Multi FV Manager Master Method

Note:
A receiver ECU receives a synchronization message from a Sender ECU which sends secured I-PDUs which the receiver wants to get. If it receives messages from multiple sender ECUs, then it receives synchronization messages from the multiple sender ECUs.

11.4.1 Definition of Freshness Value

11.4.1.1 Structure of Freshness Value

Software Component FVM provides the FV to SecOC constructed from separate counters in the following structure:

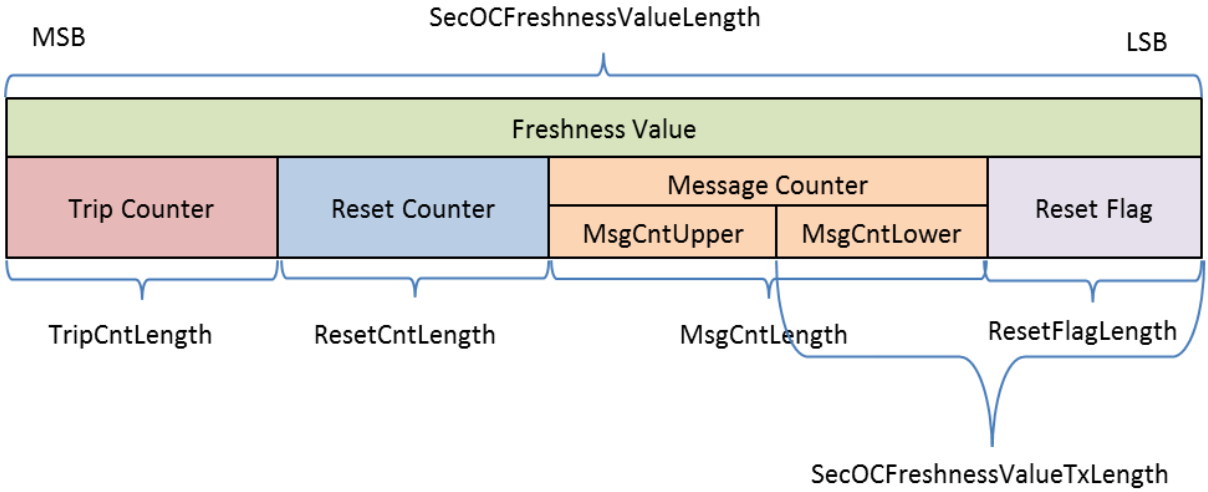

Figure 21: Structure of FreshnessValue

Data	***Description***
Trip Counter (TripCnt)	This counter is incremented in units of trips by the FV management master ECU. With the single FV management master method, the FV management master ECU sends a new TripCnt as the synchronization message (TripResetSyncMsg) to the sender ECU and receiver ECU. All the sender and receiver ECUs maintain this value. With the multi FV management master method, the sender ECU sends a new TripCnt as the synchronization message to the receiver ECU. The receiver ECU maintains this value.
Reset counter (ResetCnt)	This counter is incremented periodically by the FV management master ECU on the cycle configured by ResetCycle. With the single FV management master method, the FV management master ECU sends a new ResetCnt as the synchronization message (TripResetSyncMsg) to the sender ECU and receiver ECU. All of the sender and receiver ECUs maintain this value. With the multi FV management master method, the sender ECU sends a new ResetCnt as the synchronization message to the receiver ECU. The receiver ECU maintains this value.
Message counter (MsgCnt)	This counter is incremented with every message transmission by the sender ECU. It is managed for each secure message by the sender ECU.

	"MsgCntLower" refers to the range that is included in the truncated freshness value for Message Counter transmission (inside SecOCFreshnessValueTxLength). "MsgCntUpper" refers to the range that is not included in the truncated freshness value for Message Counter transmission (outside SecOCFreshnessValueTxLength).
Reset Flag (ResetFlag)	This flag is updated in synchronization with the reset counter. It is the ResetFlagLength(bit) value from the lower end of the reset counter.

Table 3 - Structure of Freshness Value

Abbreviation	*Description*
ResetCycle	Reset counter increment cycle
TripCntLength	Full length of the trip counter (bit)
ResetCntLength	Full length of the reset counter (bit)
MsgCntLength	Full length of the message counter (bit)
ResetFlagLength	Length of the reset flag (bit)
ClearAcceptanceWindow	Permissible range for a counter initialization when the trip counter reaches the maximum value. Under the erroneous situation such as miss-synchronous counter between FV master and slave around upper limit of trip counter, this window parameter would work effectively to recover the situation as a robustness. To understand further mechanism, see clause 11.4.1.2.

Table 4 – Abbreviation of FVM variable

11.4.1.2 Specification of counters used to construct Freshness Value

Counter	*Increment condition*	*Initialization condition*	*Initial value*	*Counter length*
Trip counter (TripCnt)	- When the FV management master ECU starts - On wakeup - On reset - When the power status changes: "IG-OFF⇒IG-ON", incremented by 1	The increment conditions occur at the maximum value of the trip counter.	FV management master ECU: 1 Slave ECU: 0	TripCntLength Max 24 bit
Reset counter (ResetCnt)	Incremented by 1 at regular time intervals (ResetCycle)	The trip counter is incremented or initialized.	FV management master ECU: 1 Slave ECU: 0	ResetCntLength Max 24bit
Message counter (MsgCnt)	Increment 1 value for each message transmission	The reset counter is incremented or initialized.	Slave ECU: 0	MsgCntLength Max 48 bit

Reset Flag (ResetFlag)	- (It follows the reset counter, as it is the ResetFlagLength(bit) value from the lower end of the reset counter.)	ResetFlagLength Max 2bit

Table 5 - Behavior of counters used to construct freshness value

Note: The Length of Freshness Value (SecOCFreshnessValueLength) cannot exceed 64 bits, so the lengths of each of the three counters (Trip Counter, Reset Counter, Message Counter) and reset flag must be adopted individually, to match this requirement that their total length does not exceed 64 bits.

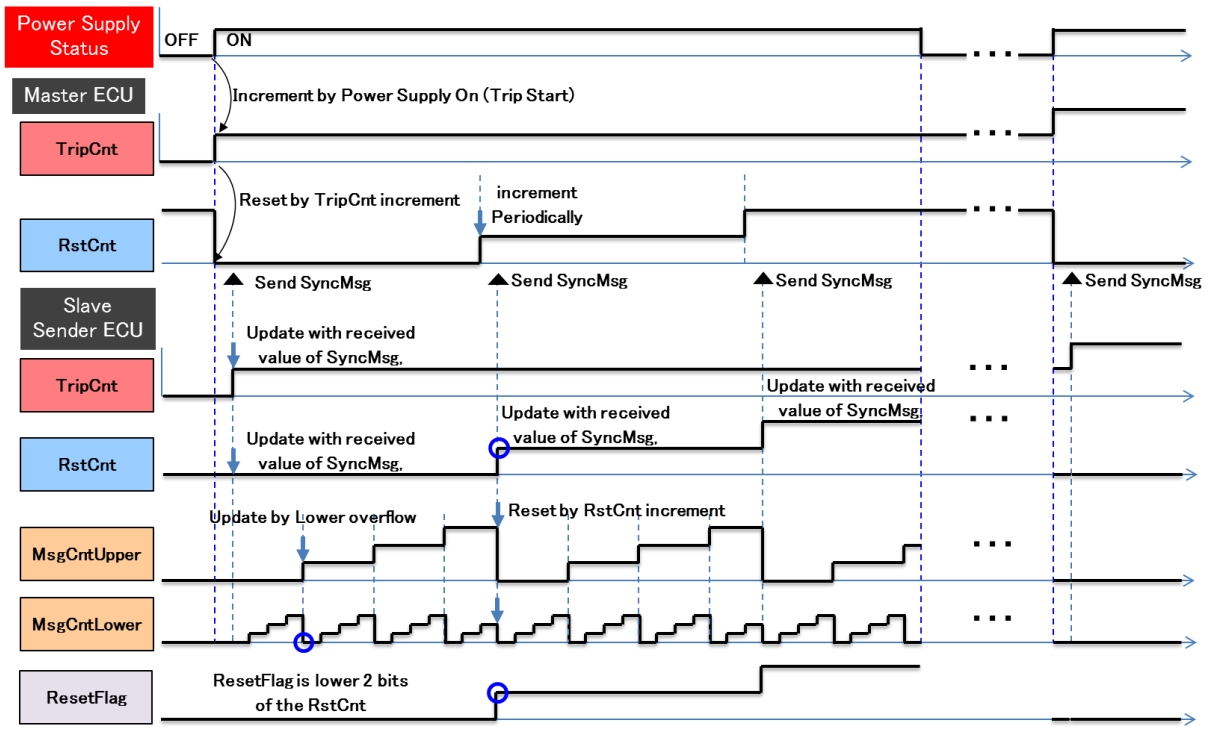

Figure 22: Behavior example of freshness value (TripCnt, RstCnt, MsgCnt, ResetFlag)

Note:
Figure 22 shows an example of the case where "ResetFlagLength is 2 bits, and MsgCntLower is 2 bits". Be careful to design the counter values whose maximum is never reached in order to prevent attacks such as replay.
If each of the counters that constitute the freshness value reaches its maximum value, the following procedures are taken. In addition, the slave ECU notifies the upstream module that the message counter value has reached the maximum value.
[Reason] Even when one of the counters that constitute the freshness value reaches its maximum value, it may still be desirable to continue the communication.
[Reason] When any counter reaches its maximum value, replay attacks can no longer be detected.

1. FV management master ECU

- At the maximum value of the trip counter
  When an increment condition of the trip counter occurs at the maximum value of the trip counter, the trip counter and the reset counter are returned to their initial values. The synchronization message is sent even after the trip counter is returned to the initial value.

- At the maximum value of the reset counter
  When an increment condition of the reset counter occurs at the maximum value of the reset counter, the reset counter is fixed to the maximum value.
  The synchronization message is sent even at the maximum value of the reset counter. Even though FV is still overflowed notifying to upper layer application or diagnostic system, there are some use case which wants to continue to communicate with other ECUs under limited circumstance. For the purpose of synchronization with the Slave ECU, FV Master is fixing the counter value on the upper limit to wait for re-sync from Slave ECU side, thus master ECU periodically try to send TripResetSyncMsg with fixed RstCnt until re-sync succeeds.

2. Slave ECU

- At the maximum value of the trip counter
  If both Conditions 1 and 2 below are established, the synchronization message is received and authenticator verification is performed.
  If the verification result is OK, the latest values of the trip counter and reset counter are updated with the received trip counter and reset counter values.
  In addition, the previously sent value and previously received value of each counter are returned to the initial values.

  Condition 1:
  “Maximum value of the trip counter” – “ClearAcceptanceWindow”
  ≤ “Latest value of the trip counter maintained by the slave ECU”
  ≤ “Maximum value of the trip counter”

  Condition 2:
  “Initial value of the trip counter”
  ≤ “Trip counter value in the synchronization message”
  ≤ “Initial value of the trip counter” + “ClearAcceptanceWindow”

  [Reason] This is to provide a permissible range (ClearAcceptanceWindow), taking into consideration cases where the trip counters of the FV management master ECU and slave ECU deviate from each other around the maximum value.
  The initial value of the trip counter in Condition 2 refers to the initial value of the FV management master ECU.

- At the maximum value of the reset counter
  The sender ECU generates an authenticator by fixing the message counter to the maximum value.
  The receiver ECU verifies the authenticator by overwriting the message counter with the maximum value.

- At the maximum value of the message counter
  The sender ECU generates an authenticator by fixing the message counter to the maximum value.
  The receiver ECU verifies the authenticator by overwriting the message counter with the maximum value.

11.4.2 Synchronization Message Format

The FV management master ECU and slave ECU handle the synchronization messages that comply with the following format.

Note:
The message used to synchronize the trip counter with the reset counter is sent from the FV management master ECU to the slave ECU. It is desirable to use the same message for the trip counter and reset counter.

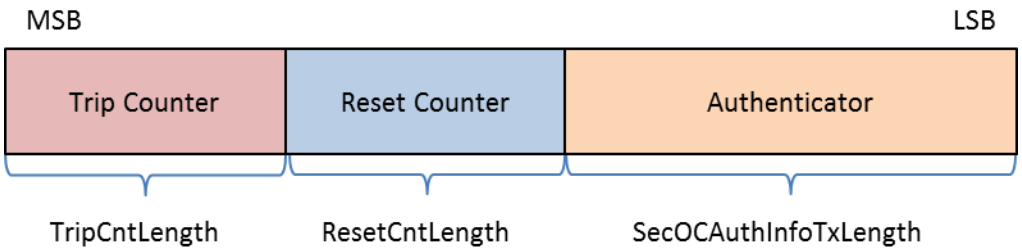

Figure 23: Format of the synchronization message (TripResetSyncMsg)

11.4.3 Processing of FV Management Master

11.4.3.1 Processing of Initialization

The FV management master ECU performs the following processes at ECU startup, on wakeup or ECU reset.

- Obtain the trip counter value that is stored in the nonvolatile memory.
  Set the trip counter to the initial value at the first startup.
- Set the reset counter to the initial value.

When the trip counter value cannot be read from the non-volatile memory, any failsafe value can be used as the trip counter and reset counter until the next trip counter update.

When the trip counter is incremented, the FV management master ECU stores the incremented value to the nonvolatile memory. It might be better that the trip counter is stored in secure flash to prevent from malicious manipulation as an option, using RAM buffering. However, storing the failsafe value into the non-volatile memory shall not be implemented.

Note:
Even when the trip counter changes from the maximum value to the initial value (see clause 11.4.1.2), it is treated as an increment and is stored in the non-volatile memory.

11.4.3.2 Sending of Synchronization Message

The FV management master ECU sends the trip counter and reset counter that it manages to the slaveECU periodically (every ResetCycle). However, if they can be sent at startup, it sends them immediately.

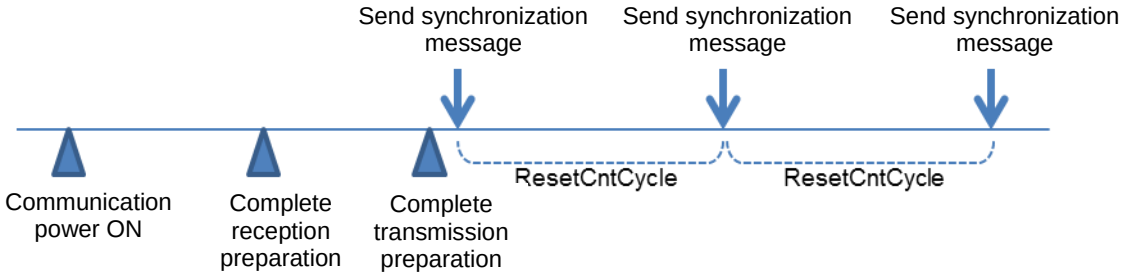

Figure 24: Transmission Timing of Synchronization Message

11.4.4 Processing of Slave ECUs

Software Component Freshness Value Manager [FVM] shall implement and store the following design values for counters:

Design Value	***Description***	***Update condition***
Trip Counter (TripCnt)	Latest Trip Counter value received successfully from FV management master ECU.	Successful reception of TripResetSyncMsg
Reset Counter (ResetCnt)	Latest Reset Counter value received successfully from FV management master ECU	Successful reception of TripResetSyncMsg
Freshness Value (FV)	Freshness Value maintained for each message to be secured. The structure of FV is according to Figure 21. Transmission message: Before a Secured I-PDU is sent (when SecOC requests FV to be provided), it	SecOC notification of the start of Secured I-PDU transmission or, SecOC notification of successful MAC verification

	holds the value used in the transmission of the previous Secured I-PDU. After it is sent (when SecOC sends a notification of the transmission of the Secured I-PDU), the value is updated with the value provided to SecOC for transmission. Reception message: Before a Secured I-PDU is received (when SecOC requests FV to be provided), it holds the value used for verification at the reception of the previous Secured I-PDU. After it is received (when SecOC sends a notification of successful MAC verification), the value is updated with the value provided to SecOC for reception.	

Table 6 - Design Value for Counter

.

Explanation:

- Latest Trip Counter or Reset Counter refers to the values received from FV management master ECU
- Previous Trip Counter, Reset Counter, Message Counter and Reset Flag refers to the individual freshness values used for previous authentication generation or verification.
- Received Reset Flag or Message Counter refers to truncated freshness value used to build the Authentication Information as described by SecOC.

Trip Counter and Reset Counter provided by FV management master ECU and stored by FVM.

Trip Counter [TripCnt] **Latest**	Reset Counter [ResetCnt] **Latest**

Figure 25: Trip Counter and Reset Counter

Freshness Value for each secured I-PDU that is provided to SecOC by FVM and it consists of Trip Counter, Reset Counter, Message Counter, Reset Flag.

Trip Counter [TripCntPdu] **Previous**	Reset Counter [ResetCntPdu] **Previous**	Message Counter [MsgCnt] **Previous**	Reset Flag [ResetFlag] **Previous**
Freshness Value [FV] For each secured message. It holds the value used for previous transmission or reception of a secured I-PDU.			

Table 7 – Freshness Value for each secured message

11.4.4.1 Processing of Initialization

The slave ECU performs the following processes at ECU startup, on wakeup or ECU reset.

- Obtain the trip counter value that is stored in the non-volatile memory, and then set it to the latest value.
  Set the initial value to the latest value of the trip counter at the first startup, or when the trip counter value cannot be read from the non-volatile memory.
- Set the latest value of the reset counter to the initial value.
- Set all the previously sent values and previously received values to the initial values.

Note:
The latest value of the trip counter has been saved in the non-volatile memory. Both latest and previous trip value in volatile memory are initialized based on the trip counter in the non-volatile memory. In this context, the previous value refers to the previously sent value for the sender ECU, or the previously received value for the receiver ECU.

11.4.4.2 Receiving of Synchronization Message

When the synchronization message is received, the slave ECU performs the following processes to complete the synchronization process.

1. SecOC obtains the freshness value for verification from FVM. FVM compares the freshness value in the method described in [UC_SecOC_00200], and constructs the freshness value for verification, because it is assumed that the trip counter value and reset counter value in the synchronization message (TripResetSyncMsg) are sent and received at full length.

2. SecOC constructs the authentication data, which consists of "Message ID | Freshness value".

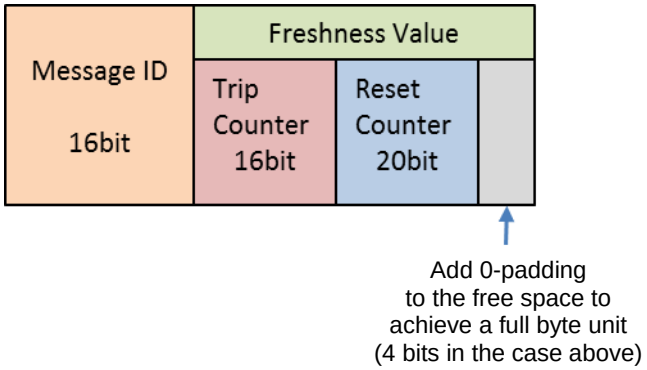

Figure 26: Example of Authentication Data Structure of Synchronization Message (TripResetSyncMsg)

3. SecOC verifies the authenticator and notifies FVM of the verification result. If the verification result is OK, FVM updates the received trip counter value and reset

counter value as the latest values. SecOC also notifies the application of the received trip counter value and reset counter value.

4. If the verification result fails (NG), SecOC does not perform re-verification, but notifies the application and discards the reception message.

Note:
When the trip counter is incremented, the application stores the incremented value to the non-volatile memory. It is preferable that the value is stored securely. However, storing the failsafe value into the non-volatile memory shall not be implemented. Even when the trip counter changes from the maximum value to the initial value (see clause 11.4.1.2), it is treated as an increment and is stored in the non-volatile memory.

11.4.4.3 Construction of Freshness Value for Transmission

When SecOC requests to obtain the freshness value for transmission, FVM constructs the freshness value for transmission according to Table 8.

Trip Counter | Reset Counter comparison (*1)	Construction of Freshness Value for Transmission			
	Trip Counter	Reset Counter	Message Counter	Reset Flag
Latest value= Previously sent value	Previously sent value	Previously sent value	Previously sent value +1	The ResetFlagLength(bit) value from the lower end of the reset counter (previously sent value)
Latest value ≠ Previously sent value	Latest value	Latest value	Inittial Value +1	The ResetFlagLength(bit) value from the lower end of the reset counter (latest value)
*1 - Compare the latest values and previously sent values of the trip counter and reset counter. The "|" symbol means a connection.				

Table 8 - Construction of Freshness Value (FV) for Tx

When SecOC sends a transmission start notification, FVM maintains the constructed freshness value for transmission (trip counter, reset counter, message counter) as the previously sent value.

11.4.4.4 Construction of Freshness Value for Reception

When SecOC requests to obtain the freshness value for verification, FVM constructs the freshness value for verification according to Table 9, based on the following three results.

1. Reset flag comparison (see Figure 29)
2. Trip counter and reset counter comparison
3. Message counter (lower end) comparison

Construction Format	Condition			Construction of freshness value for verification			
	(1) Reset flag comparison	(2) Trip counter | reset counter comparison	(3) Message counter (lower end) comparison (*3)	Trip Counter	Reset Counter	Message Counter (Upper) (*1)	Message Counter (Lower) (*2)
Format 1	Latest value =	Latest value =	Previously received value <	Previously	Previously	Previously	Received

	Received value	Previously received value	Received value (no carry)	Received value	Received value	Received value	value
Format 2			Previously received value >= Received value (with carry)	Previously Received value	Previously Received value	Previously received value+1	Received value
Format 3		Latest value > Previously received value	-	Latest value	Latest value	0	Received value
Format 1	Latest value-1 = Received value	Latest value-1 = Previously received value	Previously received value < Received value (no carry)	Previously Received value	Previously Received value	Previously Received value	Received value
Format 2			Previously received value >= Received value (with carry)	Previously Received value	Previously Received value	Previously received value+1	Received value
Format 3		Latest value-1 > Previously received value	-	Latest value	Latest value-1	0	Received value
Format 1	Latest value+1 = Received value	Latest value+1 = Previously received value	Previously received value < Received value (no carry)	Previously Received value	Previously Received value	Previously Received value	Received value
Format 2			Previously received value >= Received value (with carry)	Previously Received value	Previously Received value	Previously received value+1	Received value
Format 3		Latest value+1 > Previously received value	-	Latest value	Latest value+1	0	Received value
Format 1	Latest value-2 = Received value	Latest value-2 = Previously received value	Previously received value < Received value (no carry)	Previously Received value	Previously Received value	Previously Received value	Received value
Format 2			Previously received value >= Received value (with carry)	Previously Received value	Previously Received value	Previously received value+1	Received value
Format 3		Latest value-2 > Previously received value	-	Latest value	Latest value-2	0	Received value
Format 1	Latest value+2 = Received value	Latest value+2 = Previously received value	Previously received value < Received value (no carry)	Previously Received value	Previously Received value	Previously Received value	Received value
Format 2			Previously received value >= Received value (with carry)	Previously Received value	Previously Received value	Previously received value+1	Received value
Format 3		Latest value+2 > Previously received value	-	Latest value	Latest value+2	0	Received value

Note:
(*1) "Message counter (Upper)" refers to the range that is not included in the freshness value of the message counter for transmission.
(*2) "Message counter (Lower)" refers to the range that is included in the freshness value of the message counter for transmission.
(*3) Compare the previously received value of the "message counter (Lower)" with the received value, and determine if carry was produced.

Table 9 - Construction of Freshness Value (FV) for Rx

The sequence for constructing the freshness value for verification, and the reset flag comparison method are as follows.

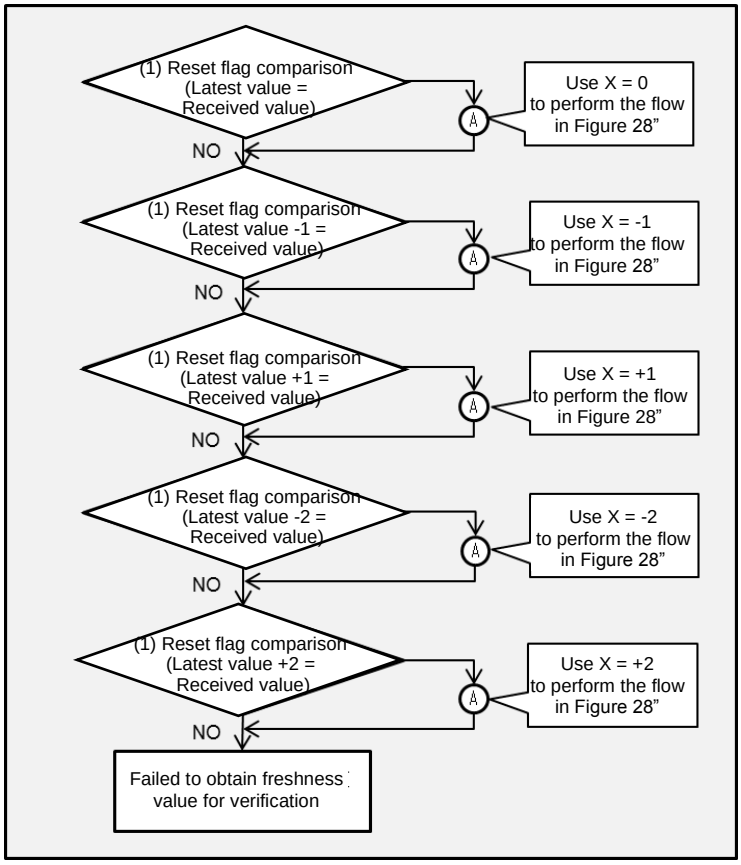

Figure 27: Construction Order of Freshness Value for Verification 1

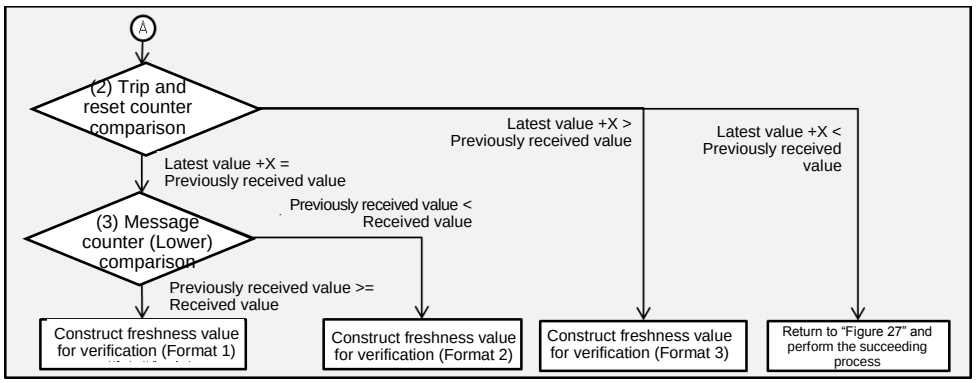

Figure 28: Construction Order of Freshness Value for Verification 2

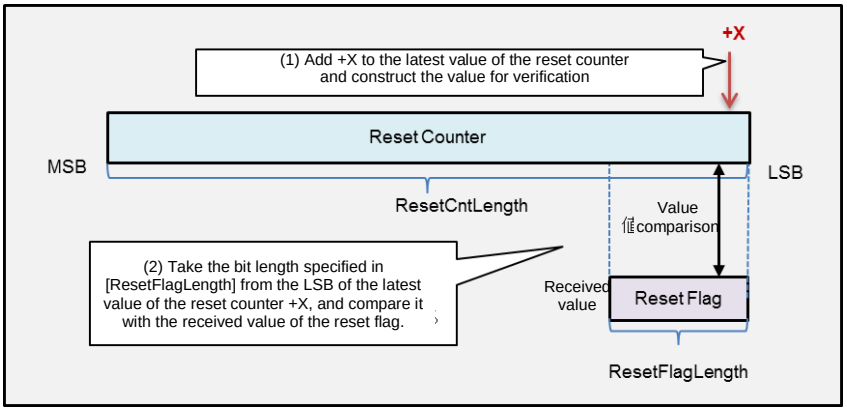

Figure 29: Reset Flag Comparison Method

SecOC uses the obtained freshness value for verification to construct authentication data and perform authenticator verification. If the verification result fails (NG), SecOC re-constructs the freshness value for verification and performs re-verification.
For the method of constructing the freshness value for verification, see Figure 27.
When SecOC sends a notification of the verification result (verification = OK), FVM maintains the constructed freshness value for verification as the previously received value.

A Not applicable requirements

[SWS_SecOC_00999]⌈These requirements are not applicable to this specification.⌋(SRS_BSW_00004, SRS_BSW_00005, SRS_BSW_00006, SRS_BSW_00007, SRS_BSW_00009, SRS_BSW_00010, SRS_BSW_00158, SRS_BSW_00160, SRS_BSW_00161, SRS_BSW_00162, SRS_BSW_00164, SRS_BSW_00167, SRS_BSW_00168, SRS_BSW_00170, SRS_BSW_00172, SRS_BSW_00300, SRS_BSW_00302, SRS_BSW_00304, SRS_BSW_00305, SRS_BSW_00306, SRS_BSW_00307, SRS_BSW_00308, SRS_BSW_00309, SRS_BSW_00310, SRS_BSW_00312, SRS_BSW_00314, SRS_BSW_00318, SRS_BSW_00321, SRS_BSW_00325, SRS_BSW_00327, SRS_BSW_00328, SRS_BSW_00330, SRS_BSW_00331, SRS_BSW_00333, SRS_BSW_00334, SRS_BSW_00335, SRS_BSW_00336, SRS_BSW_00339, SRS_BSW_00341, SRS_BSW_00342, SRS_BSW_00343, SRS_BSW_00346, SRS_BSW_00347, SRS_BSW_00360, SRS_BSW_00361, SRS_BSW_00371, SRS_BSW_00374, SRS_BSW_00375, SRS_BSW_00377, SRS_BSW_00378, SRS_BSW_00379, SRS_BSW_00380, SRS_BSW_00383, SRS_BSW_00388, SRS_BSW_00389, SRS_BSW_00390, SRS_BSW_00392, SRS_BSW_00393, SRS_BSW_00394, SRS_BSW_00395, SRS_BSW_00396, SRS_BSW_00397, SRS_BSW_00398, SRS_BSW_00399, SRS_BSW_00400, SRS_BSW_00401, SRS_BSW_00405, SRS_BSW_00406, SRS_BSW_00408, SRS_BSW_00409, SRS_BSW_00410, SRS_BSW_00411, SRS_BSW_00412, SRS_BSW_00413, SRS_BSW_00416, SRS_BSW_00417, SRS_BSW_00419, SRS_BSW_00422, SRS_BSW_00423, SRS_BSW_00424, SRS_BSW_00427, SRS_BSW_00428, SRS_BSW_00429, SRS_BSW_00432, SRS_BSW_00433, SRS_BSW_00437, SRS_BSW_00438, SRS_BSW_00439, SRS_BSW_00440, SRS_BSW_00441, SRS_BSW_00447, SRS_BSW_00448, SRS_BSW_00451, SRS_BSW_00452, SRS_BSW_00453, SRS_BSW_00454, SRS_BSW_00456, SRS_BSW_00458, SRS_BSW_00459, SRS_BSW_00460, SRS_BSW_00461, SRS_BSW_00462, SRS_BSW_00463, SRS_BSW_00464, SRS_BSW_00465, SRS_BSW_00466, SRS_BSW_00467, SRS_BSW_00469, SRS_BSW_00470, SRS_BSW_00471, SRS_BSW_00472)