Elektrobit

EB tresos® AutoCore Generic 8

SECOC documentation

release notes update for the SecOC module

product release 8.8.7

Elektrobit Automotive GmbH
Am Wolfsmantel 46
91058 Erlangen, Germany
Phone: +49 9131 7701 0
Fax: +49 9131 7701 6333
Email: info.automotive@elektrobit.com

Technical support

https://www.elektrobit.com/support

Legal disclaimer

Confidential information.

All brand names, trademarks, and registered trademarks are property of their rightful owners and are used only for description.

Table of Contents

1. Overview

This document provides you with the release notes to accompany an update to the `SecOC` module. Refer to the changelog Section 2.1, “Change log” for details of changes made for this update.

Release notes details

- EB tresos AutoCore release version: 8.8.7
- EB tresos Studio release version: 29.2.1
- AUTOSAR R4.3 Rev 0
- Build number: B587955

2. SecOC module release notes

- AUTOSAR R4.3 Rev 0
- AUTOSAR SWS document version: 4.3.0
- Module version: 2.8.7.B587955
- Supplier: Elektrobit Automotive GmbH

2.1. Change log

This chapter lists the changes between different versions.

Module version 2.8.7

2022-12-06

- Internal module improvement. This module version update does not affect module functionality

Module version 2.8.6

2022-11-25

- Internal module improvement. This module version update does not affect module functionality

Module version 2.8.5

2022-10-31

- ASCSECOC-809 Fixed known issue: No reattempt of verification for PDU collection after reception of replacing PDU

Module version 2.8.4

2022-10-28

- Internal module improvement. This module version update does not affect module functionality

Module version 2.8.3

2022-09-16

- Internal module improvement. This module version update does not affect module functionality

Module version 2.8.2

2022-08-19

- ASCSECOC-794 Fixed known issue: Secured PDU header functionality not available
- ASCSECOC-795 Fixed known issue: SecOC_VerifyStatusOverride() not available
- Implemented the option to send secured PDU with default authentication information

Module version 2.8.1

2022-06-10

- Added a container named EB General to hold general EB specific configuration parameters
- Implemented support for signature based authentication
- Implemented re-authentication for Tx authentic PDU

Module version 2.8.0

2022-05-13

- Extended the SecOC_VerifyStatusOverride feature to be also compliant with AUTOSAR R20-11 specification
- Extended the SecOCReceptionOverflowStrategy feature to also support the queuing of PDUs functionality
- Implemented the handling of dynamic length PDUs
- Extended the SecOC_VerificationStatusService feature to be also compliant with AUTOSAR R20-11 specification
- Implemented multicore feature according to AUTOSAR R20-11
- Improved Rx state machine
- Implemented the handling of MetaData for queued secured PDUs
- Improved the file inclusion hierarchy and restructured RX/TX data types
- Enhanced the parameter descriptions from Tresos with detailed explanations and links to dependencies
- Reduced configuration time by removing SecOcCsmMode

- Reworked Rx side exclusive area
- ASCSECOC-759 Fixed known issue: Wrong data transmitted on SecOC_TriggerTransmit()
- Implemented the "Ignore verification result" feature for FVM failures

Module version 2.7.7

2022-02-18

- Internal module improvement. This module version update does not affect module functionality

Module version 2.7.6

2021-10-08

- Add support for the usecase: SecOC_StartOfReception is called with TpSduLength = 0

Module version 2.7.5

2021-08-20

- ASCSECOC-579 Fixed known issue: Compile error occurs if only Tx or Rx are configured and EB make files are not used

Module version 2.7.4

2021-06-25

- ASCSECOC-562 Fixed known issue: The SecOC calls APIs of other modules in an interrupt context and/or exclusive area

Module version 2.7.3

2021-03-05

- Internal module improvement. This module version update does not affect module functionality

Module version 2.7.2

2021-02-12

- ASCSECOC-512 Fixed known issue: Authentic PDU is passed to the upper layer with wrong values

Module version 2.7.1

2021-01-22

- Internal module improvement. This module version update does not affect module functionality

Module version 2.7.0

2020-12-18

- Implemented callout function which provides the ability to change the Csm job ID during the run time

Module version 2.6.5

2020-10-23

- Removed issue generated duo to the missing undef for TS_RELOCATABLE_CFG_ENABLE
- ASCSECOC-414 Fixed known issue: Upper layer authentic Tx PDU is not accepted until SecOC is done processing the current PDU with the same ID

Module version 2.6.4

2020-06-19

- ASCSECOC-371 Fixed known issue: The cryptographic Tx PDU can contain a wrong message link
- ASCSECOC-380 Fixed known issue: The cryptographic Tx PDU can contain an incomplete message link
- Implemented option for auto-mapping of the main functions
- Changed NO_INIT memory sections to CLEARED
- Improved the Tx side state machine handling

Module version 2.6.3

2020-05-22

- Improved the xdm file by moving EB custom configuration parameter from the "General" tab to "EB General" tab

- ASCSECOC-374 Fixed known issue: SecOC can send unintended messages if the bypass mechanism is activated

Module version 2.6.2

2020-04-24

- Updated file name from SecOC_PBCfg.c to SecOC_PBcfg.c.

Module version 2.6.1

2020-03-27

- Implemented the mechanism to bypass the authentication routine during runtime.
- ASCSECOC-367 Fixed known issue: New authentic Tx PDU(s) are not being accepted in case the Tx Confirmation was not given

Module version 2.6.0

2020-02-21

- Implemented the SecOCSameBufferPduCollection option to link a collection of PDUs to use a buffer.

Module version 2.5.2

2020-01-23

- Extended the custom verification status propagation

Module version 2.5.1

2019-12-06

- Improved module handling by splitting source code in Rx/Tx separate files

Module version 2.5.0

2019-10-11

- ASCSECOC-334 Fixed known issue: Synchronous processing of the Rx PDU is interrupted when the verification result is negative

Module version 2.4.2

2019-09-06

- Implemented the option to propagate MAC verification return code to the application

Module version 2.4.1

2019-08-09

- Implemented support for RTE with FunctionElision = TRUE

Module version 2.4.0

2019-06-14

- Improved the SecOC state machine handling

Module version 2.3.2

2019-06-07

- Implemented option to propagate the MAC generate status when the service was successful or not

Module version 2.3.1

2019-05-17

- Improved the Csm job IDs handling
- Implemented synchronous Pdu processing for Rx and Tx side

Module version 2.3.0

2019-02-15

- Implemented option to skip the verification procedure by calling SecOC_VerifyStatusOverride with the overrideStatus parameter set to 43. In the case where the SecOCRxSecuredPduLayer configuration parameter is set to SecOCRxSecuredPduCollection, the lower layer authentic PDU is forwarded directly to the upper layer without waiting for the corresponding cryptographic PDU.
- Implemented the reception overflow strategies REJECT and REPLACE

Module version 2.2.3

2019-01-25

- ASCSECOC-301 Fixed known issue: Server call to Freshness Management SWC is incorrectly modeled for multi-partition systems
- ASCSECOC-302 Fixed known issue: Buffer overflow occurs if freshness values are smaller than 57 bits in multi-partition systems

Module version 2.2.2

2018-11-23

- ASCSECOC-297 Fixed known issue: Wrong compiler abstraction macro used for function parameter's pointer class
- ASCSECOC-298 Fixed known issue: Buffer overflow in case of small authenticator length

Module version 2.2.1

2018-10-26

- Updated the description for some of the configuration parameters and external functions

Module version 2.2.0

2018-09-28

- Implemented support for post build selectable
- Improved the configuration phase, when SecOCSecuredRxPduVerification is off, no Csm jof reference needs to be selected for SecOCRxAuthServiceConfigRef.
- Extended the usecases when SecOC_GetRxFreshnessAuthData() is called by the SecOC module, this function will be called if the freshness value length of the PDU is 0 bits or the length of the authentic data that needs to be send to freshness value SWC is not 0 bits

Module version 2.1.11

2018-07-27

- ASCSECOC-278 Fixed known issue: Out-of-bounds access if full freshness value length is not a multiple of 8 bits and truncated MAC length is smaller than one byte

Module version 2.1.10

2018-06-22

- Implemented the GetRxFreshnessAuthData and GetTxFreshnessTruncData functions and all the related functionality.
- ASCSECOC-271 Fixed known issue: Link error if no PDU is configured with SecOCPduType = SECOC_TPPDU
- Updated the use of exclusive areas

Module version 2.1.9

2018-05-25

- ASCSECOC-262 Fixed known issue: Wrong return type for function SecOC_SPduTxConfirmation
- Implemented the option to skip the configuration of SecOCFreshnessValueFuncName and SecOCSecuredPDUTransmittedFuncName when the freshness value length is equal to 0.
- Implemented support for callout functions which are indicating the SWC/CDD that the MAC Generate procedure has failed.
- Implemented support to configure an default MAC which shall be used when the MAC could not be generated
- Extended the function SecOC_VerifyStatusOverride to be able to override the Csm_MacVerify return value and callback result to "Pass".
- Implemented support for DataId length up to 32 bits.
- Implemented support for SecOCPduType SECOC_TPPDU

Module version 2.1.8

2018-04-20

- ASCSECOC-256 Fixed known issue: IMPLEMENTATION_CONFIG_VARIANT is not enabled
- Implemented support for PduLengthType of 32 bits
- Implemented support for secured PDU collection

Module version 2.1.7

2018-03-16

- Adapted the memory sections for runnable entities declared by the Rte

Module version 2.1.6

2018-02-16

- ASCSECOC-225 Fixed known issue: For multiple PDUs with the same SecOCFreshnessValueId, SecOC overrides status only for one PDU
- Implemented support for configuration of the Csm mode for every PDU configured in SecOC
- Implemented support for callout functions which are updating the secured PDU layout

Module version 2.1.5

2018-01-19

- Implemented the configuration parameter SecOCEnableForcedPassOverride and the related functionality
- Changed Primitive Implementation Data Types to Redefinition Implementation Data Types for unspecified Implementation Data Types
- Implemented the skip verification for secured PDU
- Implemented support for secured area within a Pdu

Module version 2.1.4

2017-12-15

- ASCSECOC-208 Fixed known issue: SecOC does not forward the PDUs to the upper layer regardless of the verification result when the configuration option SecOcIgnoreVerificationResult is enabled
- Implemented the TxConfirmation timeout
- ASCSECOC-212 Fixed known issue: If processing is not finished, the PDU length is overwritten by incoming PDU

Module version 2.1.3

2017-11-17

- Improved the SecOC authentication processing regarding the Tx confirmation

Module version 2.1.2

2017-10-20

- ASCSECOC-185 Fixed known issue: Wrong return type in SecOC function definition of Csm callback
- Improved the checking in the validation schema for the Csm jobs referenced by the SecOC module for I-PDU authentication and verification
- ASCSECOC-188 Fixed known issue: Compile error occurs if only Tx or Rx are configured with asynchronous Csm

Module version 2.1.1

2017-10-09

- ASCSECOC-159 Fixed known issue: Undefined macro CSM_E_VER_OK
- ASCSECOC-162 Fixed known issue: Message verification fails because the authenticator generated on Tx side is always 0
- Updated the SecOC configuration schema to AUTOSAR 4.3
- Implemented support for asynchronous Csm mode
- ASCSECOC-181 Fixed known issue: Out of bounds read access occurs if an Rx PDU has freshness length 0

Module version 2.1.0

2017-08-28

- ASCSECOC-106 Fixed known issue: Wrong calculation of truncated Tx freshness value bits
- Implemented support for triggered transmission

Module version 2.0.0

2017-08-04

- ASCSECOC-119 Fixed known issue: Inclusion of Rte_SecOC.h within SecOC.h creates compiler error
- ASCSECOC-87 Fixed known issue: Automatic calculation of PDU IDs using the Handle ID wizard does not work
- ASCSECOC-92 Fixed known issue: Authentic PDU is considered for upper layer for If and Tp module
- ASCSECOC-142 Fixed known issue: SecOC expects a Tx confirmation even if the lower layer module does not accept the transmission request
- ASCSECOC-100 Fixed known issue: SecOC does not compile if configuration parameter PduRCancelTransmit is set to false

- Implemented support for multiple secured I-PDUs with same freshness value ID
- Updated the interface operations GetRxFreshness and GetTxFreshness according to the requirement SWS_SecOC_91002 of the AUTOSAR 4.3
- Updated the type SecOC_VerificationStatusType with the element SecOCDataID according to the requirement SWS_SecOC_00160 of the AUTOSAR 4.3
- Implemented support for multiple Secured I-PDUs with the same DataIds
- ASCSECOC-133 Fixed known issue: Wrong calculation of Tx-secured PDU size for buffer clearing
- Update SecOC to use Csm synchronous single call Autosar 4.3 API

Module version 1.2.0

2017-04-03

- Added RfC 73691, configuration parameter SecOcIgnoreVerificationResult
- Implemented optional interface to query the freshness value from an external source (SWC or CDD)
- Implemented Bugzilla RfC 73692: Splitting the SecOC main function into an Rx- and an Tx-Path
- ASCSECOC-99 Fixed known issue: `SecOC` uses incorrect PDU ID for the Rx authentic layer PDU

Module version 1.1.0

2015-10-15

- Added ISO-C90 compatible interfaces for APIs SecOC_FreshnessValueWrite() and SecOC_FreshnessValueRead()

Module version 1.0.1

2015-06-19

- Corrected usage of the AUTOSAR memory mapping

Module version 1.0.0

2015-04-28

- Initial release for `SecOC` which supports a basic feature set

2.2. New features

- `Send the secured PDU with default authentication information`: The `SecOC` module provides the option to send out secured PDUs with default authentication information in case the freshness values retrieving failed or the MAC generation failed on the sender side.

2.3. Elektrobit-specific enhancements

This chapter lists the enhancements provided by the module.

- `DataId` length up to 32 bits

  Description:

  The length for the used `DataId` can be configured for 8 bits, 16 bits or 32 bits.

  Rationale:

  The configuration of the length of the DataId allows more flexibility for the project defining the `DataIds` to be used.
- Overriding return value of MAC verification

  Description:

  The `SecOC` module provides the opportunity to override the return value of function `Csm_MacVerify` and its related callback result to "Pass" for a given number of PDUs with the same Freshness Value ID. This feature is available if SecOCEnableForcedPassOverride is set to TRUE. It is an extension to the functionality of `SecOC_VerifyStatusOverride`.

  Rationale:

  This enhancement can be used during development to authenticate PDUs also during temporary errors from the hardware used to calculate the MACs.
- Default authenticator

  Description:

  The `SecOC` module provides the configuration parameter `SecOCDefaultAuthenticatorValue`. If this parameter is enabled, and MAC generation fails, SecOC sends a secured PDU containing a default authenticator with the value defined by the configuration parameter.

  Rationale:

This enhancement enables sending secured PDUs during development, if the generation of MACs is not available.

- Indication of MAC generation result

  Description:

  Using the configuration parameter `SecOCMacGenerateStatusPropagationMode` the `SecOC` can propagate the status of the MAC generation to the application.

  Rationale:

  The propagation of the MAC generation result together with the feature for propagation of the MAC verification result enables the application to get all information about the current status and health of the secure onboard communication.

- Secured PDU layout callout

  Description:

  The `SecOC` provides the opportunity to configure callout functions which are called before sending and after receiving a secured PDU. These functions can be used to correct the bus layout for secured PDUs.

  Rationale:

  This enhancement can be used e.g. to add or remove padding bytes for dynamic length PDUs which require a static length on the bus (e.g. CAN-FD).

- TxConfirmation timeout

  Description:

  `SecOC` provides the configuration parameter `SecOCTxConfirmationTimeout`. It can be used to define a maximum time the `SecOC` waits for a TxConfirmation from the lower layer during transmission. If no TxConfirmation was indicated until the timeout has expired, `SecOC` continues processing the next PDU.

  Rationale:

  This enhancement is a robustness feature to stabilize the bus communication.

- Support of *Calculate Handle IDs* wizard

  Description:

  The `SecOC` module supports the calculation of handle IDs with the *Calculate Handle IDs* wizard.

  Rationale:

  With this feature you can configure handle IDs of secured and authenticated PDUs in the `SecOC` module.

- Configuration parameter SecOCCryptoBitLength

  Description:

  The SecOC module provides the additional configuration parameter SecOCCryptoBitLength. If this parameter is enabled, the SecOC module passes the length information for the MAC in bits to the authentication service. If this parameter is disabled, the SecOC module passes the length information for the MAC in bytes to the authentication service.

  Rationale:

  This configuration parameter allows you to configure the SecOC module to the needs of the used cryptographic primitives.

- Configuration parameter SecOCASR403

  Description:

  The SecOC module provides the additional configuration parameter SecOCASR403. If this parameter is enabled, the SecOC module provides the interfaces to the PduR module as specified by AUTOSAR 4.0.3. If this parameter is disabled, the SecOC module provides the interfaces to the PduR module as specified by AUTOSAR 4.2.1.

  Rationale:

  This configuration parameter allows you to integrate SecOC module together with an AUTOSAR 4.0.3 PduR module as well as with an AUTOSAR 4.2.1 PduR module.

- Configuration parameter SecOCRteUsage

  Description:

  The SecOC module provides the additional configuration parameter SecOCRteUsage. If this parameter is enabled, the SecOC provides and uses interfaces to the Rte. If this parameter is disabled, the SecOC module does not provide or use the interfaces to the Rte. Per default SecOCRteUsage is disabled.

  Rationale:

  The Rte interface is not necessarily required for the usage of the SecOC module. The SecOC interface to the Rte represents a feature of the SecOC module. This feature can be used if required, but can also be disabled to reduce the code size.

2.4. Deviations

This chapter lists the deviations of the module from the AUTOSAR standard.

- No support of SecOC_ChangeParameter

Description:

The SecOC module does not provide the ability to change a specific transport protocol parameter (e.g. block size).

Rationale:

The SecOC_ChangeParameter mechanism is not supported by the SecOC module.

Requirements:

SWS_SecOC_91011, SWS_SecOC_00218, SWS_SecOC_00103

- No support of SecOC_CancelReceive

  Description:

  The SecOC module does not provide the ability to cancel an ongoing reception of a PDU in a lower layer transport protocol module.

  Rationale:

  The SecOC_CancelReceive mechanism is not supported by the SecOC module.

  Requirements:

  SWS_SecOC_91010, SWS_SecOC_00217

- No support of development error detection

  Description:

  The SecOC module neither provides development errors nor calls the Det module. The deviation also includes all related parameters and functionalities.

  Rationale:

  The development error detection mechanism is not supported by the SecOC module.

  Requirements:

  SWS_SecOC_00155, SWS_SecOC_00101, SWS_SecOC_00102, SWS_SecOC_00164, SWS_SecOC_00166, ECUC_SecOC_00007, SWS_SecOC_00138, SWS_SecOC_00251, SWS_SecOC_00248

- Deviation of file structure

  Description:

  The file structure of the SecOC module deviates from the file structure provided by the AUTOSAR specification.

  - The `SecOC` module does not include the file `Dem.h`.
  - Not all type definitions are defined in `SecOC_Types.h`. However, type definitions are available if `SecOC.h` is included.

  Rationale:

  - The `SecOC` module does not include the file `Dem.h`, because production errors are not defined.
  - Not all type definitions are defined in `SecOC_Types.h`, because several type definitions are configuration-dependent.

  Requirements:

  SWS_SecOC_00002

- Secured I-PDUs can have DataId with the same value

  Description:

  The parameter `SecOCDataId` defines a numerical identifier for the Secured I-PDU. This identifier can be used for multiple Secured I-PDUs.

  Rationale:

  The `SecOC` module support multiple Secured I-PDUs with the same `SecOCDataId` value.

  Requirements:

  ECUC_SecOC_00030, ECUC_SecOC_00014

- Invalid requirement

  Description:

  Requirement SWS_SecOC_00049 is not feasible.

  Rationale:

  See https://www.autosar.org/bugzilla/show_bug.cgi?id=77622

  Requirements:

  SWS_SecOC_00049

- Interfaces to the PduR

  Description:

  The names of the interfaces to the `PduR` do not completely match the names defined in the AUTOSAR_SWS_SecureOnboardCommunication of AUTOSAR version 4.3. Because the `PduR` module is the only module to use these interfaces, this deviation has no impact usage of the SecOC. SecOC registers its interface names to the PduR and the PduR uses the provided interface names. The SecOC module provides and uses the PduR API defined by AUTOSAR version 4.0.3 or version 4.2.1 respectively.

- `SecOC_IfTxConfirmation` is named `SecOC_TxConfirmation`
- `SecOC_IfTransmit` is named `SecOC_Transmit`
- `SecOC_TpTransmit` is named `SecOC_Transmit`
- `SecOC_IfCancelTransmit` is named `SecOC_CancelTransmit`
- `SecOC_TpCancelTransmit` is named `SecOC_CancelTransmit`
- `PduR_SecOCTransmit` is named `PduR_SecOCTpTransmit` when using TP protocol
- `PduR_SecOCIfCancelTransmit` is named `PduR_SecOCCancelTransmit`
- `PduR_SecOCTpCancelTransmit` is named `PduR_SecOCCancelTransmit`
- `PduR_SecOCIfRxIndication` is named `PduR_SecOCRxIndication`

Rationale:

The interface names shall not be changed to be backward compatible.

Requirements:

SWS_SecOC_00063, SWS_SecOC_00072, SWS_SecOC_00076, SWS_SecOC_00080, SWS_SecOC_00086 SWS_SecOC_00087, SWS_SecOC_00137, SWS_SecOC_00081, SWS_SecOC_00112, SWS_SecOC_00113, SWS_SecOC_00126, SWS_SecOC_00130, SWS_SecOC_91008, SWS_SecOC_91009

- No support of Security Profiles

  Description:

  The SecOC does not support Security Profiles for security reasons. Nevertheless the configuration parameters of SecOC can be configured to match the given Security Profiles.

  Rationale:

  The risk is high, that a given Security Profile is not secure anymore in the near future, if e.g. a cryptographic algorithm is broken or a bigger key length is required to ensure security. Therefore it is highly recommended to do a security analysis on each individual use case and chose the SecOC parameters along with state of the art at the time.

  Requirements:

  SWS_SecOC_00190, SWS_SecOC_00191, SWS_SecOC_00192, SWS_SecOC_00193, SWS_SecOC_00194

- Names of Freshness Callout functions

Description:

The names of the callout functions `SecOC_GetRxFreshness` and `SecOC_GetTxFreshness` are not fix as defined by AUTOSAR_SWS_SecureOnboardCommunication. The names can be defined by the configuration parameters `SecOCFreshnessValueFuncName`.

Rationale:

The Prefix SecOC_ for a function, which is not defined by the `SecOC`, but another CDD or integration code violates the AUTOSAR rules.

Requirements:

SWS_SecOC_91004, SWS_SecOC_91007

- No support of configuration parameter `SecOCUseTxConfirmation`

  Description:

  The configuration parameter `SecOCUseTxConfirmation` is not available. It is always considered as TRUE.

  Rationale:

  `SecOCUseTxConfirmation` is an unsupported configuration parameter.

  Requirements:

  ECUC_SecOC_00085

- No support of configuration parameter `SecOCMaxAlignScalarType`

  Description:

  The configuration parameter `SecOCMaxAlignScalarType` is not available.

  Rationale:

  The type definition resulting from the configuration parameter `SecOCMaxAlignScalarType` is not used for `SecOC` of AUTOSAR version 4.3 and therefore the configuration parameter is obsolete.

  Requirements:

  ECUC_SecOC_00047

2.5. Limitations

This chapter lists the limitations of the module. Refer to the module references chapter *Integration notes*, subsection *Integration requirements* for requirements on integrating this module.

- Synchronous Pdu processing only available for synchronous Csm mode

  Description:

  Synchronous Pdu processing is not supported in case Csm is configured to execute in asynchronous mode.

  Rationale:

  Synchronous Pdu processing is blocking until the Pdu is processed completely. Thus, it shall not be available if SecOC waits for an asynchronous Csm call to return.

- SameBufferPduCollection not supported in combination with

  Description:

  The Rx same buffer PDU collection cannot be used with the Rx secured PDU collection (SecOCRxSecuredPduLayer = SecOCRxSecuredPduCollection) or with SecOCReceptionOverflowStrategy set to REPLACE.

  Rationale:

  The above combination are not supported because the reception procedure would require a strict scheduling of the different PDUs that are using the same buffer.

2.6. Open-source software

`SecOC` does not use open-source software.