Elektrobit

EB tresos® AutoCore Generic 8 CSM and CRYIF documentation

release notes update for the CryIf 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 `CryIf` 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: B602344

2. CryIf module release notes

- AUTOSAR R4.3 Rev 0
- AUTOSAR SWS document version: 4.3.0
- Module version: 1.0.36.B602344
- Supplier: Elektrobit Automotive GmbH

2.1. Change log

This chapter lists the changes between different versions.

Module version 1.0.35

2022-10-28

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

Module version 1.0.34

2022-09-16

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

Module version 1.0.33

2022-07-22

- Changed INIT_BOOLEAN memory sections to INIT_8

Module version 1.0.32

2022-05-13

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

Module version 1.0.31

2022-04-01

- Added AUTOSAR 4.4.0 API and ARXML compatibility.

Module version 1.0.30

2022-02-18

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

Module version 1.0.29

2021-12-10

- Added new APIs CryIf_KeySetInvalid() and CryIf_KeyGetStatus() based on ASR R20-11.

Module version 1.0.27

2021-10-08

- Removed the dependency to the not mandatory CommonPublishedInformation.

Module version 1.0.26

2021-09-17

- Fixed incorrect query of VendorApiInfix and VendorId.

Module version 1.0.25

2021-08-20

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

Module version 1.0.24

2021-06-25

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

Module version 1.0.23

2021-04-30

- ASCCRYIF-169 Fixed known issue: CryIf causes unexpected data inconsistencies if CryIf_KeyElementCopy is used for keys which are located in different Crypto drivers.
- Added support for EB tresos HandleIdWizards.

Module version 1.0.22

2021-01-22

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

Module version 1.0.21

2020-12-18

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

Module version 1.0.20

2020-10-23

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

Module version 1.0.19

2020-09-25

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

Module version 1.0.18

2020-07-31

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

Module version 1.0.17

2020-02-21

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

Module version 1.0.16

2020-01-24

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

Module version 1.0.15

2019-12-06

- Added configuration parameter to switch between CryIf 4.3.0 and 4.3.1 API and ARXML compatibility and improved API and ARXML compatibility in general. Also this configuration parameter provides the possibility to choose the mixed 4.3.0 and 4.3.1 EB style API and ARXML version that is necessary for old EB Csm modules less than version 3.1.0 and EB Crypto modules less than version 2.0.0.
- Internal module improvement. This module version update does not affect module functionality.

Module version 1.0.14

2019-10-11

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

Module version 1.0.13

2019-08-09

- ASCCRYIF-103 Fixed known issue: CryIf does not generate symbolic names for CryIfChannels and CryIfKeys
- ASCCRYIF-104 Fixed known issue: CryIf does not use symbolic names for referenced CryptoDriverObjects and CryptoKeys

Module version 1.0.12

2019-06-19

- Added creation of Crypto API Module implementation prefix based on BSWMDs in addition to the default creation based on CommonPublishedInformations.

Module version 1.0.11

2019-05-17

- Removed 'myEcuParameterDefinition' from XDM and BMD file.
- ASCCRYIF-101 Fixed known issue: DESTINATION-REFs in the VSMD violate TPS_ECUC_06015

Module version 1.0.10

2019-01-25

- Changed return values of CryIf_KeyElementCopy() and CryIf_KeyCopy() to CRYPTO_E_KEY_SIZE_-MISMATCH instead of E_NOT_OK when the key element sizes do not match, as discussed in https://bugzilla.autosar.org/show_bug.cgi?id=79493 and realized in R4.4.

Module version 1.0.9

2018-10-26

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

Module version 1.0.8

2018-06-22

- Improved robustness of CryIf_ProcessJob() and CryIf_CancelJob() regarding invalid key IDs

Module version 1.0.7

2018-05-25

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

Module version 1.0.6

2018-04-06

- ASCCRYIF-67 Fixed known issue: The KeyCopy / KeyElementCopy functions fail to copy key elements
- ASCCRYIF-71 Fixed known issue: Incorrect check of referenced functions in KeyDerive, KeyCopy, KeyElementCopy and CertificateVerify

Module version 1.0.5

2018-03-16

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

Module version 1.0.4

2018-02-16

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

Module version 1.0.3

2017-12-20

- Corrected compiler warnings
- Improved robustness of multi-instantiation of Crypto Drivers regarding Crypto preconfiguration and relative x-paths

Module version 1.0.2

2017-11-17

- Updated limitations and documentation

Module version 1.0.1

2017-10-02

- ASCCRYIF-18 Fixed known issue: Number of configurable keys and channels is limited to 32
- ASCCRYIF-16 Fixed known issue: CryIf_ProcessJob() and CryIf_CancelJob() pass CryIf channel ID instead of Crypto driver object ID to Crypto API
- ASCCRYIF-15 Fixed known issue: CryIf routes Csm API calls to wrong Crypto modules and/or CryptoDriverObjects and/or CryptoKeys

Module version 1.0.0

2017-08-04

- Implemented CryIf module compliant to the AUTOSAR 4.3 specification

2.2. New features

- `CryIf_KeySetInvalid` API: The module supports the ASR R20-11 CryIf_KeySetInvalid API and provides the option to set the state of a key to invalid through `CryIf_KeySetInvalid`.
- `CryIf_KeyGetStatus` API: The module supports the ASR R20-11 CryIf_KeyGetStatus API and provides the option to obtain the status of a key through `CryIf_KeyGetStatus`.

2.3. Elektrobit-specific enhancements

This chapter lists the enhancements provided by the module.

- This module provides no Elektrobit-specific enhancements.

2.4. Deviations

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

- Range check of job->cryIfKeyId and job->cryIfTargetKeyId

  Description:

  The Elektrobit CryIf does not check the range of the mentioned Crypto_JobType members for dispatching key IDs in the context of key Id dispatching, but job->jobPrimitiveInputOutput->cryIfKeyId and job->jobPrimitiveInputOutput->targetCryIfKeyId

  Rationale:

  - This is incorrectly specified by AUTOSAR.

  Requirements:

  - AUTOSAR 4.4.0:

    SWS_CryIf_00134, SWS_CryIf_00135
- Key element checks

  Description:

  The Elektrobit CryIf does not process any key element related checks.

  Rationale:

  - Possible checks are incorrectly specified by AUTOSAR.

  https://jira.autosar.org/browse/AR-111507

  Requirements:

  - AUTOSAR 4.4.0:

    SWS_CryIf_00138

- Default value FALSE for CryIfDevErrorDetect and CryIfVersionInfoApi

  Description:

  The Elektrobit CryIf specifies the default value of the configuration parameters CryIfDevErrorDetect and CryIfVersionInfoApi to FALSE.

  Rationale:

  - AUTOSAR does not specify an default value.

  Requirements:

  - AUTOSAR 4.3.0:

    ECUC_CryIf_00010, ECUC_CryIf_00011
  - AUTOSAR 4.3.1:

    ECUC_CryIf_00010, ECUC_CryIf_00011
- CryIf_KeyCopy() does not call Crypto_<vi>_<ai>_KeyElementCopy()

  Description:

  The Elektrobit CryIf does not call Crypto_<vi>_<ai>_KeyElementCopy() within its API CryIf_KeyCopy().

  Rationale:

  - https://jira.autosar.org/browse/AR-3644

  Requirements:

  - AUTOSAR 4.3.0:

    SWS_CryIf_00119
  - AUTOSAR 4.3.1:

    SWS_CryIf_00119
- Development error detection of Crypto Driver

  Description:

  The Elektrobit CryIf does not report Development errors depending on whether the development error detection for the Crypto Driver is enabled.

  Rationale:

  - This is incorrectly specified by AUTOSAR.

  Requirements:

  - AUTOSAR 4.3.0:

    SWS_CryIf_00053
  - AUTOSAR 4.3.1:

    SWS_CryIf_00053

- Development Error Type CRYPTO_E_PARAM_HANDLE

  Description:

  The Elektrobit CryIf does not report the development error type CRYPTO_E_PARAM_HANDLE to the DET, but CRYIF_E_PARAM_HANDLE.

  Rationale:

  - Possible checks are incorrectly specified by AUTOSAR.

    https://jira.autosar.org/browse/AR-111508

  Requirements:

  - AUTOSAR 4.4.0:

    SWS_CryIf_00134, SWS_CryIf_00135, SWS_CryIf_00138

- Direction of parameter 'versioninfo' of CryIf_GetVersionInfo()

  Description:

  The direction of parameter 'versioninfo' of CryIf_GetVersionInfo() is OUT.

  Rationale:

  - The direction of parameter 'versioninfo' of CryIf_GetVersionInfo() is incorrectly specified to IN.

  Requirements:

  - AUTOSAR 4.3.0:

    SWS_CryIf_91001

  - AUTOSAR 4.3.1:

    SWS_CryIf_91001
  - AUTOSAR 4.4.0:

    SWS_CryIf_91001
- Return values of CryIf_ProcessJob()

  Description:

  The return values CRYIF_E_QUEUE_FULL and CRYIF_E_SMALL_BUFFER of CryIf_ProcessJob() are replaced by CRYPTO_E_QUEUE_FULL and CRYPTO_E_SMALL_BUFFER.

  Rationale:

  - The return values for 'Request failed, the queue is full' and 'The provided buffer is too small to store the result' of CryIf_ProcessJob() are incorrectly specified to CRYIF_E_QUEUE_FULL and CRYIF_E_SMALL_BUFFER.

  Requirements:

  - AUTOSAR 4.3.0:

    SWS_CryIf_91003
- Return values of CryIf_KeyElementCopy()

  Description:

  The return value CRYPTO_E_KEY_EXTRACT_DENIED of CryIf_KeyElementCopy() is not supported.

  Rationale:

  - The return value for 'Request failed, not allowed to extract key element' of CryIf_KeyElementCopy() is specified via CRYPTO_E_KEY_EXTRACT_DENIED and CRYPTO_E_KEY_READ_FAIL. But only CRYPTO_E_KEY_READ_FAIL is specified as an extension to Std_ReturnType.

  Requirements:

  - AUTOSAR 4.3.0:

    SWS_CryIf_91015
- CryIfKeyId does not start from zero

  Description:

  CryIfKeyId shall be consecutive, gapless and shall start from zero.

  Rationale:

  - This requirement is not applicable. It's invalidated by note 'The Ids in the configuration containers shall be consecutive, gapless and shall start from zero'.

  Requirements:

  - AUTOSAR 4.3.0:

    ECUC_CryIf_00007
  - AUTOSAR 4.3.1:

    ECUC_CryIf_00007

- CryIfChannelId does not start from zero

  Description:

  CryIfChannelId shall be consecutive, gapless and shall start from zero.

  Rationale:

  - This requirement is not applicable. It's invalidated by note 'The Ids in the configuration containers shall be consecutive, gapless and shall start from zero'.

  Requirements:

  - AUTOSAR 4.3.0:

    ECUC_CryIf_00004
  - AUTOSAR 4.3.1:

    ECUC_CryIf_00004

- Return value of CryIf_KeyCopy() and CryIf_KeyElementCopy()

  Description:

  The functions CryIf_KeyCopy() and CryIf_KeyElementCopy() now return CRYPTO_E_KEY_SIZE_MISMATCH instead of E_NOT_OK when the key element sizes do not match.

  Rationale:

  - https://jira.autosar.org/browse/AR-57986

  Requirements:

  - AUTOSAR 4.3.0:

SWS_CryIf_00115, SWS_CryIf_00121

- AUTOSAR 4.3.1:

  SWS_CryIf_00115, SWS_CryIf_00121

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.

- Job Cancellation Interface: CryIf_CancelJob() expects Crypto Drivers with the following Crypto_CancelJob API: Std_ReturnType Crypto_CancelJob(uint32 objectId, Crypto_JobType* job). Also see RfC 80287.

2.6. Open-source software

`CryIf` does not use open-source software.