MICROSAR CryIf

Technical Reference

Crypto Interface

Version 1.2.0

Authors	Markus Schneider, Philipp Ritter
Status	Released

Document Information

History

Author	Date	Version	Remarks
Schneider, Markus	2017-03-07	1.01.00	Initial creation of Technical Reference
Ritter, Philipp	2017-05-08	1.02.00	Changed chapter 5.1.6, 5.1.7, 5.1.8, 5.1.11

Reference Documents

No.	Source	Title	Version
[1]	AUTOSAR	AUTOSAR_SWS_CryptoInterface.pdf	4.3.0
[2]	AUTOSAR	AUTOSAR_SWS_DET.pdf	4.3.0

Contents

© 2017 Vector Informatik GmbH

© 2017 Vector Informatik GmbH

Illustrations

Tables

1 Component History

The component history gives an overview over the important milestones that are supported in the different versions of the component.

Component Version	New Features
1.00.00	Initial beta release
1.01.00	Adaptions to the specification; several improvements and bug fixes
1.02.00	Release of component

Table 1-1 Component history

2 Introduction

This document describes the functionality, API and configuration of the AUTOSAR BSW module CRYIF as specified in [1].

Supported AUTOSAR Release*:	4.3	
Supported Configuration Variants:	pre-compile	
Vendor ID:	CRYIF_VENDOR_ID	30 decimal (= Vector-Informatik, according to HIS)
Module ID:	CRYIF_MODULE_ID	112 decimal (according to ref. [1])

* For the detailed functional specification please also refer to the corresponding AUTOSAR SWS.

The Crypto Interface (CRYIF) is called by the Cryptographic Service Manager (CSM) to forward its service requests to the underlying Crypto Drivers (CRYPTO). The CRYIF has access to the CRYPTO to calculate results with their cryptographic services. These results are returned to the CSM by the CRYIF.

2.1 Architecture Overview

The following figure shows where the CRYIF is located in the AUTOSAR architecture.

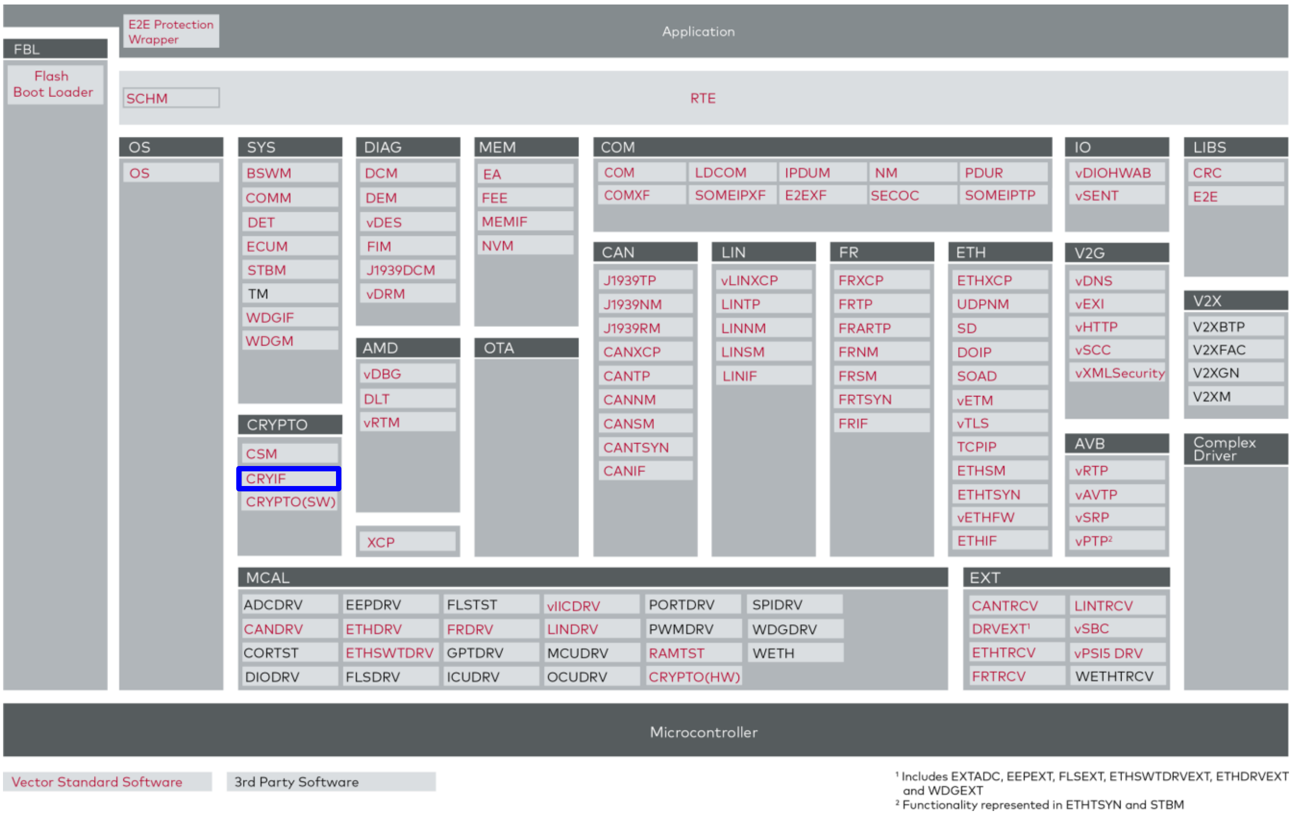

Figure 2-1 AUTOSAR 4.3 Architecture Overview

The next figure shows the interfaces to adjacent modules of the CRYIF. These interfaces are described in chapter 5.

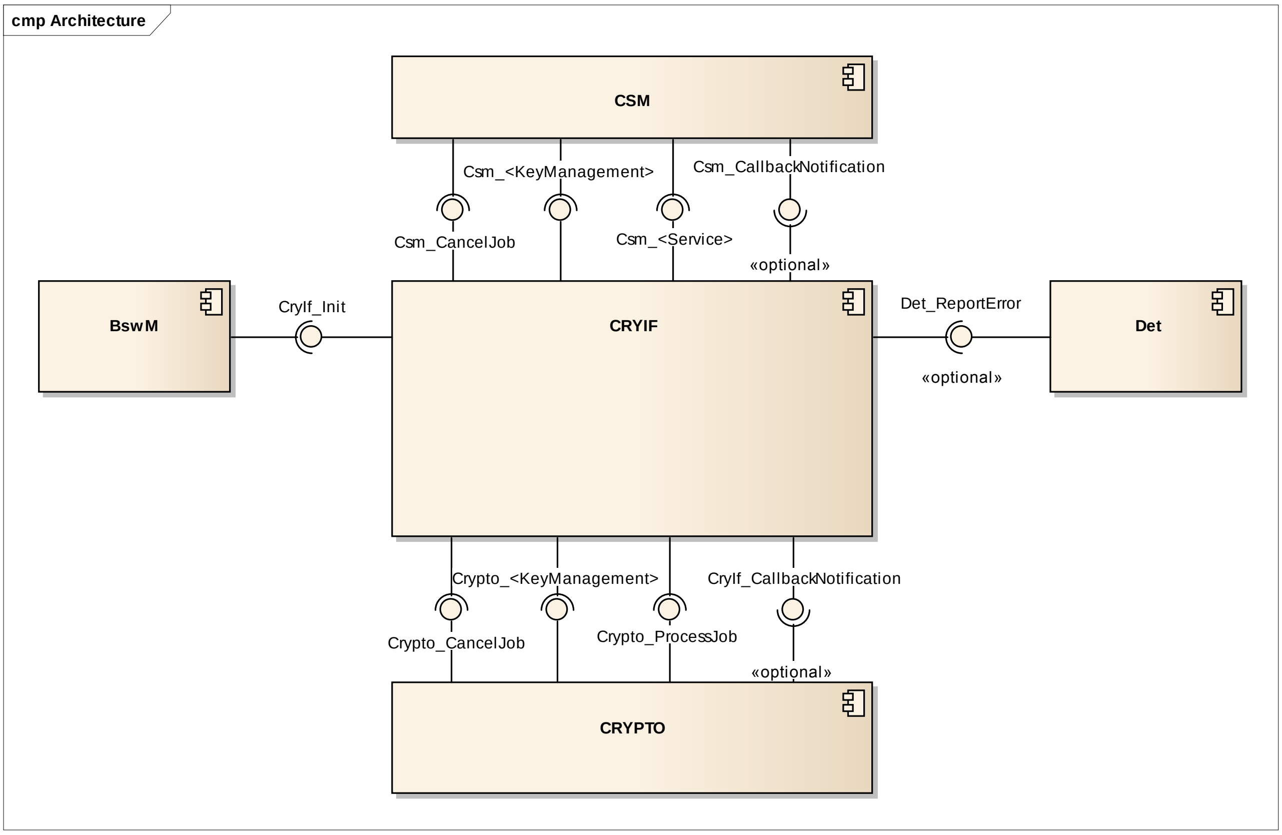

Figure 2-2 Interfaces to adjacent modules of the CRYIF

3 Functional Description

3.1 Features

The features listed in the following tables cover the complete functionality specified for the CRYIF.

The AUTOSAR standard functionality is specified in [1], the corresponding features are listed in the tables

- Table 3-1 Supported AUTOSAR standard conform features

The following features specified in [1] are supported:

Supported AUTOSAR Standard Conform Features
Dispatching jobs to the configured Crypto Driver
Dispatching key management functionalities
Forward Callback Notification

Table 3-1 Supported AUTOSAR standard conform features

3.2 Initialization

Before any other functionality of the CRYIF module can be called the initialization function `CryIf_Init()` has to be called by the BSWM.

For manual null initialization of RAM variables the CRYIF offers the function `CryIf_InitMemory()` which can be called before the `CryIf_Init()`.

3.3 States

The CRYIF does not have a state machine.

3.4 Main Functions

CRYIF does not provide a main function. All calls are synchronous.

3.5 Error Handling

3.5.1 Development Error Reporting

By default, development errors are reported to the DET using the service `Det_ReportError()` as specified in [2], if development error reporting is enabled (i.e. pre-compile parameter `CRYIF_DEV_ERROR_REPORT==STD_ON`).

If another module is used for development error reporting, the function prototype for reporting the error can be configured by the integrator, but must have the same signature as the service `Det_ReportError()`.

The reported CRYIF ID is 112.

© 2017 Vector Informatik GmbH

The reported service IDs identify the services which are described in 5.1. The following table presents the service IDs and the related services:

Service ID	Service
0x00	CryIf_Init
0x01	CryIf_GetVersionInfo
0x02	CryIf_ProcessJob
0x03	CryIf_CancelJob
0x04	CryIf_KeyElementSet
0x05	CryIf_KeySetValid
0x06	CryIf_KeyElementGet
0x0f	CryIf_KeyElementCopy
0x10	CryIf_KeyCopy
0x07	CryIf_RandomSeed
0x08	CryIf_KeyGenerate
0x09	CryIf_KeyDerive
0x0A	CryIf_KeyExchangeCalcPubVal
0x0B	CryIf_KeyExchangeCalcSecret
0x0C	CryIf_CertificateParse
0x11	CryIf_CertificateVerify

Table 3-2 Service IDs

The errors reported to DET are described in the following table:

Error Code	Description
0x00	API service used without module initialization
0x01	Initialization of CRYIF module failed
0x02	API request called with invalid parameter (null pointer)
0x03	API request called with invalid parameter (out of range)
0x04	API request called with invalid parameter (invalid value)
0x11	The service CryIf_Init() is called while the module is already initialized

Table 3-3 Errors reported to DET

4 Integration

This chapter gives necessary information for the integration of the MICROSAR CRYIF into an application environment of an ECU.

4.1 Scope of Delivery

The delivery of the CRYIF contains the files which are described in the chapters 4.1.1 and 4.1.2:

4.1.1 Static Files

File Name	Description
CryIf.c	This file contains the CRYIF source code.
CryIf.h	This is the header file of the CRYIF.
CryIf_Cbk.h	This is the callback header file of CRYIF.

Table 4-1 Static files

4.1.2 Dynamic Files

The dynamic files are generated by the configuration tool DaVinci Configurator 5 Pro

File Name	Description
CryIf_Cfg.c	This is configuration source file.
CryIf_Cfg.h	This is configuration header file.

Table 4-2 Generated files

5 API Description

For an interfaces overview please see Figure 2-2.

5.1 Services provided by CRYIF

5.1.1 CryIf_InitMemory

Prototype	
void **CryIf_InitMemory** (void)	
Parameter	
void	none
Return code	
void	none
Functional Description	
Power-up memory initialization.	
Particularities and Limitations	
Use this function in case these variables are not initialized by the startup code. Module is uninitialized. Initialize component variables at power up.	
Call context	
> TASK > This function is Synchronous > This function is Non-Reentrant	

Table 5-1 CryIf_InitMemory

5.1.2 CryIf_Init

Prototype	
void **CryIf_Init** (void)	
Parameter	
ConfigPtr [in]	Configuration structure for initializing the module
Return code	
void	none
Functional Description	
Initialization function.	
Particularities and Limitations	
Specification of module initialization > Interrupts are disabled.Module is uninitialized.CryIf_InitMemory has been called unless	

CryIf_ModuleInitialized is initialized by start-up code. This function initializes the module CryIf. It initializes all variables and sets the module state to initialized.
Call context
> TASK > This function is Synchronous > This function is Non-Reentrant

Table 5-2 CryIf_Init

5.1.3 CryIf_GetVersionInfo

Prototype	
`void **CryIf_GetVersionInfo** (Std_VersionInfoType *versioninfo)`	
Parameter	
versioninfo [out]	Pointer to where to store the version information. Parameter must not be NULL.
Return code	
void	none
Functional Description	
Returns the version information.	
Particularities and Limitations	
none CryIf_GetVersionInfo() returns version information, vendor ID and AUTOSAR module ID of the component.	
Call context	
> TASK|ISR2 > This function is Synchronous > This function is Reentrant	

Table 5-3 CryIf_GetVersionInfo

5.1.4 CryIf_ProcessJob

Prototype	
`Std_ReturnType **CryIf_ProcessJob** (uint32 channelId, Crypto_JobType *job)`	
Parameter	
channelId [in]	Holds the identifier of the crypto channel.
job [in,out]	Pointer to the configuration of the job. Contains structures with user and primitive relevant information.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.

	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
	CRYPTO_E_KEY_NOT_VALID Request failed, the key is not valid.
	CRYPTO_E_QUEUE_FULL Request failed, the queue is full.
	CRYPTO_E_SMALL_BUFFER Request failed, the provided buffer is too small to store the result.
Functional Description	
Process the received job.	
Particularities and Limitations	
none This interface dispatches the received jobs to the configured crypto driver object.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-4 CryIf_ProcessJob

5.1.5 CryIf_CancelJob

Prototype	
`Std_ReturnType` **`CryIf_CancelJob`** `(uint32 channelId, Crypto_JobType *job)`	
Parameter	
channelId [in]	Holds the identifier of the crypto channel.
job [in,out]	Pointer to the configuration of the job. Contains structures with user and primitive relevant information.
Return code	
Std_ReturnType	E_OK Request successful, job has been removed.
Std_ReturnType	E_NOT_OK Request failed, job could not be removed.
Functional Description	
Cancels the received job.	
Particularities and Limitations	
none This interface removes the provided job from the underlying Crypto Driver Object queue.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-5 CryIf_CancelJob

5.1.6 CryIf_KeyElementSet

Prototype	
Std_ReturnType **CryIf_KeyElementSet** (uint32 cryIfKeyId, uint32 keyElementId, const uint8 *keyPtr, uint32 keyLength)	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key whose key element shall be set.
keyElementId [in]	Holds the identifier of the key element which shall be set.
keyPtr [in]	Holds the pointer to the key data which shall be set as key element.
keyLength [in]	Contains the length of the key element in bytes.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
	CRYPTO_E_KEY_WRITE_FAIL Request failed, write access was denied.
	CRYPTO_E_KEY_NOT_AVAILABLE Request failed, the key is not available.
	CRYPTO_E_KEY_SIZE_MISMATCH Request failed, the key element size does not match size of provided data.
Functional Description	
Sets a key element.	
Particularities and Limitations	
none This function shall dispatch the key element set function to the configured crypto driver object.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-6 CryIf_KeyElementSet

5.1.7 CryIf_KeySetValid

Prototype	
Std_ReturnType **CryIf_KeySetValid** (uint32 cryIfKeyId)	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key whose key elements shall be set to valid.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.

Functional Description
Sets the key to valid.
Particularities and Limitations
none This function shall dispatch the key set valid function to the configured crypto driver object.
Call context
> TASK > This function is Synchronous > This function is Reentrant

Table 5-7 CryIf_KeySetValid

5.1.8 CryIf_KeyElementGet

Prototype	
`Std_ReturnType CryIf_KeyElementGet (uint32 cryIfKeyId, uint32 keyElementId, uint8 *resultPtr, uint32 *resultLengthPtr)`	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key whose key element shall be set.
keyElementId [in]	Holds the identifier of the key element which shall be set.
keyPtr [in]	Holds the pointer to the key data which shall be set as key element.
keyLength [in]	Contains the length of the key element in bytes.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
	CRYPTO_E_KEY_READ_FAIL Request failed, read access was denied.
	CRYPTO_E_KEY_NOT_AVAILABLE Request failed, the key is not available.
	CRYPTO_E_SMALL_BUFFER Request failed, the provided buffer is too small to store the result.
Functional Description	
Exports the key element	
Particularities and Limitations	
none This function shall dispatch the get key element function to the configured crypto driver object.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-8 CryIf_KeyElementGet

5.1.9 CryIf_KeyElementCopy

Prototype	
`Std_ReturnType` **`CryIf_KeyElementCopy`** `(uint32 cryIfKeyId, uint32 keyElementId, uint32 targetCryIfKeyId, uint32 targetKeyElementId)`	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key whose key element shall be the source element.
keyElementId [in]	Holds the identifier of the key element which shall be the source for the copy operation.
targetCryIfKeyId [in]	Holds the identifier of the key whose key element shall be the destination element.
targetKeyElementId [in]	Holds the identifier of the key element which shall be the destination for the copy operation.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
	CRYPTO_E_KEY_READ_FAIL Request failed, read access was denied.
	CRYPTO_E_KEY_WRITE_FAIL Request failed, write access was denied.
	CRYPTO_E_KEY_EXTRACT_DENIED Request failed, not allowed to extract key material.
	CRYPTO_E_KEY_NOT_AVAILABLE Request failed, the key is not available.
	CRYPTO_E_KEY_SIZE_MISMATCH Request failed, the key element sizes are not compatible.
Functional Description	
Copy key element.	
Particularities and Limitations	
none This function shall copy a key elements from one key to a target key.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-9 CryIf_KeyElementCopy

5.1.10 CryIf_KeyCopy

Prototype
`Std_ReturnType` **`CryIf_KeyCopy`** `(uint32 cryIfKeyId, uint32 targetCryIfKeyId)`

Parameter	
cryIfKeyId [in]	Holds the identifier of the key whose key element shall be the source element.
targetCryIfKeyId [in]	Holds the identifier of the key whose key element shall be the destination element.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
	CRYPTO_E_KEY_READ_FAIL Request failed, read access was denied.
	CRYPTO_E_KEY_WRITE_FAIL Request failed, write access was denied.
	CRYPTO_E_KEY_NOT_AVAILABLE Request failed, the key is not available.
	CRYPTO_E_KEY_SIZE_MISMATCH Request failed, the key element sizes are not compatible.
Functional Description	
Copy the key.	
Particularities and Limitations	
none This function shall copy all key elements from the source key to a target key.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-10 CryIf_KeyCopy

5.1.11 CryIf_RandomSeed

Prototype	
`Std_ReturnType` **`CryIf_RandomSeed`** `(uint32 cryIfKeyId, const uint8 *seedPtr, uint32 seedLength)`	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key for which a new material shall be generated.
seedPtr [in]	Holds a pointer to the memory location which contains the data to feed the seed.
seedLength [in]	Contains the length of the seed in bytes.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
Functional Description	
Initialize the seed.	

Particularities and Limitations
none This function shall dispatch the random seed function to the configured crypto driver object.
Call context
> TASK > This function is Synchronous > This function is Reentrant

Table 5-11 CryIf_RandomSeed

5.1.12 CryIf_KeyGenerate

Prototype	
`Std_ReturnType CryIf_KeyGenerate (uint32 cryIfKeyId)`	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key which is to be updated with the generated value.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
Functional Description	
Generates a key.	
Particularities and Limitations	
none This function shall dispatch the key generate function to the configured crypto driver object.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-12 CryIf_KeyGenerate

5.1.13 CryIf_KeyDerive

Prototype	
`Std_ReturnType CryIf_KeyDerive (uint32 cryIfKeyId, uint32 targetCryIfKeyId)`	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key which is used for key derivation.
targetCryIfKeyId [in]	Holds the identifier of the key which is used to store the derived key.

Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
Functional Description	
Derives a key.	
Particularities and Limitations	
none This function shall dispatch the key derive function to the configured crypto driver object.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-13 CryIf_KeyDerive

5.1.14 CryIf_KeyExchangeCalcPubVal

Prototype	
`Std_ReturnType` **`CryIf_KeyExchangeCalcPubVal`** `(uint32 cryIfKeyId, uint8 *publicValuePtr, uint32 *publicValueLengthPtr)`	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key which shall be used for the key exchange protocol.
publicValuePtr [out]	Contains the pointer to the data where the public value shall be stored.
publicValueLengthPtr [in,out]	Holds a pointer to the memory location in which the public value length information is stored. On calling this function, this parameter shall contain the size of the buffer provided by publicValuePtr. When the request has finished, the actual length of the returned value shall be stored.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
	CRYPTO_E_SMALL_BUFFER Request failed, the provided buffer is too small to store the result.
Functional Description	
Calculation of the public value.	
Particularities and Limitations	
none This function shall dispatch the key exchange public value calculation function to the configured crypto driver object.	

Call context
> TASK > This function is Synchronous > This function is Reentrant

Table 5-14 CryIf_KeyExchangeCalcPubVal

5.1.15 CryIf_KeyExchangeCalcSecret

Prototype	
`Std_ReturnType` **`CryIf_KeyExchangeCalcSecret`** `(uint32 cryIfKeyId, const uint8 *partnerPublicValuePtr, uint32 partnerPublicValueLength)`	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key which shall be used for the key exchange protocol.
partnerPublicValuePtr [in]	Holds the pointer to the memory location which contains the partners public value.
partnerPublicValueLength [in]	Contains the length of the partners public value in bytes.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
	CRYPTO_E_SMALL_BUFFER Request failed, the provided buffer is too small to store the result.
Functional Description	
Calculation of the secret.	
Particularities and Limitations	
none This function shall dispatch the key exchange common shared secret calculation function to the configured crypto driver object.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-15 CryIf_KeyExchangeCalcSecret

5.1.16 CryIf_CertificateParse

Prototype
`Std_ReturnType` **`CryIf_CertificateParse`** `(uint32 cryIfKeyId)`

Parameter	
cryIfKeyId [in]	Holds the identifier of the key slot in which the certificate has been stored.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
Functional Description	
Parse stored certificate.	
Particularities and Limitations	
none This function shall dispatch the certificate parse function to the configured crypto driver object.	
Call context	
> TASK > This function is Synchronous > This function is Reentrant	

Table 5-16 CryIf_CertificateParse

5.1.17 CryIf_CertificateVerify

Prototype	
`Std_ReturnType` **`CryIf_CertificateVerify`** `(uint32 cryIfKeyId, uint32 verifyCryIfKeyId, Crypto_VerifyResultType *verifyPtr)`	
Parameter	
cryIfKeyId [in]	Holds the identifier of the key which shall be used to validate the certificate.
verifyCryIfKeyId [in]	Holds the identifier of the key containing the certificate, which shall be verified.
verifyPtr [out]	Holds a pointer to the memory location which will contain the result of the certificate verification.
Return code	
Std_ReturnType	E_OK Request successful.
	E_NOT_OK Request failed.
	CRYPTO_E_BUSY Request failed, Crypto Driver Object is busy.
Functional Description	
Certificate verification.	
Particularities and Limitations	
none Verifies the certificate stored in the key referenced by verifyCryptoKeyId with the certificate stored in the key referenced by cryIfKeyId.	
Call context	
> TASK	

> This function is Synchronous > This function is Reentrant

Table 5-17 CryIf_CertificateVerify

5.2 Services used by CRYIF

In the following table services provided by other components, which are used by the CRYIF are listed. For details about prototype and functionality refer to the documentation of the providing component.

Component	API
DET	Det_ReportError

Table 5-18 Services used by the CRYIF

5.3 Callback Functions

This chapter describes the callback function that is implemented by the CRYIF and can be invoked by other modules. The prototypes of the callback functions are provided in the header file `CryIf_Cbk.h` by the CRYIF.

5.3.1 CryIf_CallbackNotification

Prototype	
`void` **`CryIf_CallbackNotification`** `( Crypto_JobType *job, Std_ReturnType result )`	
Parameter	
`job`	Points to the completed job's information structure. It contains a callbackID to identify which job is finished.
`result`	Contains the result of the cryptographic operation.
Return code	
`void`	none
Functional Description	
Notifies the CRYIF about the completion of the request with the result of the cryptographic operation.	
Particularities and Limitations	
> This function is synchronous. > This function is non-reentrant.	

Table 5-19 CryIf_CallbackNotification

6 Configuration

In the CRYIF the attributes can be configured with the following tools:

- Configuration in DaVinci Configurator 5 Pro for a detailed description see 6.2

6.1 Configuration Variants

The CRYIF supports the configuration variants

- `VARIANT-PRE-COMPILE`

The configuration classes of the CRYIF parameters depend on the supported configuration variants. For their definitions please see the CryIf_bswmd.arxml file.

6.2 Configuration with DaVinci Configurator 5 Pro

6.2.1 General Properties

Attribute Name	Values Default value is typed bold	Description
CryIfVersionInfoApi	TRUE **FALSE**	Pre-processor switch to enable and disable availability of the API Crypto_GetVersionInfo(). - True: API CryIf_GetVersionInfo() is available - False: API CryIf_GetVersionInfo() is not available.
CryIfDevErrorDetect	**TRUE** FALSE	Switches the development error detection and notification on or off. - True: detection and notification is enabled. - False: detection and notification is disabled.
CryIfMaxNumberOfKeyElements	**10**	Size of the maximal amount of element within an key type of all referenced Crypto Drivers
CryIfMaxSizeOfKeyElement	**512**	Size of the largest key element of all referenced Crypto Drivers

Table 6-1 General Properties

6.2.2 Channel Properties

Attribute Name	Values Default value is typed bold	Description
CryIfChannelId		Identifier of the crypto channel
CryIfDriverObjectRef		Reference to a Crypto Driver Object

Table 6-2 Channel Properties

6.2.3 Key Properties

Attribute Name	Values Default value is typed bold	Description
CryIfKeyId		Identifier of the key.
CryIfKeyRef		This parameter refers to a crypto driver key.

Table 6-3 Key Properties

7 Glossary and Abbreviations

7.1 Glossary

Term	Description
CSM	Crypto Service Manager
CRYIF	Crypto Interface
CRYPTO	Crypto Driver

Table 7-1 Glossary

7.2 Abbreviations

Abbreviation	Description
API	Application Programming Interface
AUTOSAR	Automotive Open System Architecture
BSW	Basis Software
DEM	Diagnostic Event Manager
DET	Development Error Tracer
EAD	Embedded Architecture Designer
ECU	Electronic Control Unit
HIS	Hersteller Initiative Software
ISR	Interrupt Service Routine
MICROSAR	Microcontroller Open System Architecture (the Vector AUTOSAR solution)
PPORT	Provide Port
RPORT	Require Port
RTE	Runtime Environment
SRS	Software Requirement Specification
SWC	Software Component
SWS	Software Specification

Table 7-2 Abbreviations

8 Contact

Visit our website for more information on

- News
- Products
- Demo software
- Support
- Training data
- Addresses

www.vector.com

© 2017 Vector Informatik GmbH