

Document Title	SWS_CryptoInterface: Complete Change Documentation 4.3.0 - 4.3.1
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	695

Document Status	Final
Part of AUTOSAR Standard	Classic Platform
Part of Standard Release	4.3.1

Table of Contents

1	SWS_CryptoInterface	4
1.1	Specification Item SWS_Crylf_00009	4
1.2	Specification Item SWS_Crylf_00012	8
1.3	Specification Item SWS_Crylf_00016	9
1.4	Specification Item SWS_Crylf_00017	16
1.5	Specification Item SWS_Crylf_00027	24
1.6	Specification Item SWS_Crylf_00028	31
1.7	Specification Item SWS_Crylf_00029	38
1.8	Specification Item SWS_Crylf_00049	45
1.9	Specification Item SWS_Crylf_00050	52
1.10	Specification Item SWS_Crylf_00052	59
1.11	Specification Item SWS_Crylf_00053	66
1.12	Specification Item SWS_Crylf_00056	73
1.13	Specification Item SWS_Crylf_00057	80
1.14	Specification Item SWS_Crylf_00059	87
1.15	Specification Item SWS_Crylf_00060	94
1.16	Specification Item SWS_Crylf_00062	101
1.17	Specification Item SWS_Crylf_00063	109
1.18	Specification Item SWS_Crylf_00064	116
1.19	Specification Item SWS_Crylf_00068	123
1.20	Specification Item SWS_Crylf_00069	130
1.21	Specification Item SWS_Crylf_00070	137
1.22	Specification Item SWS_Crylf_00071	144
1.23	Specification Item SWS_Crylf_00073	151
1.24	Specification Item SWS_Crylf_00074	158
1.25	Specification Item SWS_Crylf_00076	165
1.26	Specification Item SWS_Crylf_00077	172
1.27	Specification Item SWS_Crylf_00082	179
1.28	Specification Item SWS_Crylf_00083	186
1.29	Specification Item SWS_Crylf_00084	194
1.30	Specification Item SWS_Crylf_00085	201
1.31	Specification Item SWS_Crylf_00086	208
1.32	Specification Item SWS_Crylf_00090	215
1.33	Specification Item SWS_Crylf_00091	222
1.34	Specification Item SWS_Crylf_00092	229
1.35	Specification Item SWS_Crylf_00093	236
1.36	Specification Item SWS_Crylf_00094	243
1.37	Specification Item SWS_Crylf_00098	250
1.38	Specification Item SWS_Crylf_00099	257
1.39	Specification Item SWS_Crylf_00107	264

1.40	Specification Item SWS_CryIf_00108	271
1.41	Specification Item SWS_CryIf_00110	279
1.42	Specification Item SWS_CryIf_00111	286
1.43	Specification Item SWS_CryIf_00112	293
1.44	Specification Item SWS_CryIf_00115	300
1.45	Specification Item SWS_CryIf_00116	304
1.46	Specification Item SWS_CryIf_00117	311
1.47	Specification Item SWS_CryIf_00118	318
1.48	Specification Item SWS_CryIf_00121	325
1.49	Specification Item SWS_CryIf_00122	329
1.50	Specification Item SWS_CryIf_00123	336
1.51	Specification Item SWS_CryIf_00124	343
1.52	Specification Item SWS_CryIf_00125	350
1.53	Specification Item SWS_CryIf_00126	357
1.54	Specification Item SWS_CryIf_00127	364
1.55	Specification Item SWS_CryIf_00129	371
1.56	Specification Item SWS_CryIf_00130	378
1.57	Specification Item SWS_CryIf_00131	385
1.58	Specification Item SWS_CryIf_91003	392
1.59	Specification Item SWS_CryIf_91015	394

1 SWS_CryptoInterface

1.1 Specification Item SWS_CryIf_00009

Trace References:

SRS_CryptoStack_00086

Content:

Type of error	Related error code	Value [hex]
API request called before initialisation of CRYIF module.	CRYIF_E_UNINIT	0x00
Initialisation of CRYIF module failed.	CRYIF_E_INIT_FAILED	0x01
API request called with invalid parameter (null pointer).	CRYIF_E_PARAM_POINTER	0x02
API request called with invalid parameter (out of range).	CRYIF_E_PARAM_HANDLE	0x03
API request called with invalid parameter (invalid value).	CRYIF_E_PARAM_VALUE	0x04
Source key element size does not match the target key elements size.	CRYIF_E_KEY_SIZE_MISMATCH	0x05

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number

and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with "job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

1.2 Specification Item SWS_CryIf_00012

Trace References:

none

Content:

Range:	CryIf_ReturnType CRYPTO_E_BUSYCry If_Return Type.CRYPTO_E_BUSY	0x02	The service request failed because the service is still busy
	CRYPTO_E_SMALL_BUFFERCry If_Return Type.CRYPTO_E_SMALL_BUFFER	0x03	The service request failed because the provided buffer is too small to store the result
	CRYPTO_E_ENTROPY_EXHAUSTIONCry If_Return Type.CRYPTO_E_ENTROPY_EXHAUSTION	0x04	The service request failed because the entropy of the random number generator is exhausted
	CRYPTO_E_QUEUE_FULLCry If_Return Type.CRYPTO_E_QUEUE_FULL	0x05	The service request failed because the queue is full
	CRYPTO_E_KEY_READ_FAILCry If_Return Type.CRYPTO_E_KEY_READ_FAIL	0x06	 The service request failed, because key element extraction is not allowed
	CRYPTO_E_KEY_WRITE_FAILCry If_Return Type.CRYPTO_E_KEY_WRITE_FAIL	0x07	The service request failed because the writing access failed
	CRYPTO_E_KEY_NOT_AVAILABLECry If_Return Type.CRYPTO_E_KEY_NOT_AVAILABLE	0x08	The service request failed because the key is not available
	CRYPTO_E_KEY_NOT_VALIDCry If_Return Type.CRYPTO_E_KEY_NOT_VALID	0x09	The service request failed because the key is invalid.
	CRYPTO_E_KEY_SIZE_MISMATCHCry If_Return Type.CRYPTO_E_KEY_SIZE_MISMATCH	0x0A	The service request failed because the key size does not match.
	CRYPTO_E_COUNTER_OVERFLOWCry If_Return Type.CRYPTO_E_COUNTER_OVERFLOW	0x0B	The service request failed because the counter is overflowed.
	CRYPTO_E_JOB_CANCELEDCry If_Return Type.CRYPTO_E_JOB_CANCELED	0x0C	The service request failed because the Job has been canceled.
Description:	—		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77374: Postponed Crypto_CancelJob()

Problem description:

If a job cannot be canceled by `Crypto_CancelJob()` immediately, it is not clear how to proceed. The requirements say:

[SWS_Crypto_00143] If no errors are detected by Crypto Driver, the service `Crypto_CancelJob()` shall remove the job from the queue. If the job is currently processed it shall be cancelled. When cancellation of current processing is not possible due to limitations, the result shall be discarded and the callback notification shall be suppressed.

[SWS_Crypto_00144] If a job is canceled, it shall return `CRYPTO_E_JOB_CANCELED` either with the callback, when the job is an asynchronous job or as the return value of the function `Crypto_CancelJob()`, in case the job is synchronous.

The following questions arise:

- (i) Is it meant in [SWS_Crypto_00143] that (only) the notification of the finished job shall be suppressed?
- (ii) [SWS_Crypto_00144]: There is no return value `CRYPTO_E_JOB_CANCELED` of `Crypto_CancelJob()`. So what should be the return value?
- (iii) What does `Crypto_CancelJob()` return when the cancellation is not possible and it has to be postponed till the job has finished? `Crypto_CancelJob()` cannot wait till the job has finished.

Could you pl. clarify these questions?

Agreed solution:

Attached to ticket

–Last change on issue 77374 comment 7–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.3 Specification Item SWS_CryIf_00016

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_GetVersionInfo shall **raise the error report** CRYIF_E_UNINIT **to the DET** if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text

according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".

rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]

[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]

[SWS_Crypto_00057]

[SWS_Crypto_00058]

[SWS_Crypto_00059]

[SWS_Crypto_00064]

[SWS_Crypto_00067]

[SWS_Crypto_00070]

[SWS_Crypto_00142]

[SWS_Crypto_00136]

[SWS_Crypto_00137]

[SWS_Crypto_00141]

[SWS_Crypto_00123]

[SWS_Crypto_00124]

[SWS_Crypto_00125]

[SWS_Crypto_00075]

[SWS_Crypto_00076]

[SWS_Crypto_00077]

[SWS_Crypto_00078]

[SWS_Crypto_00079]

[SWS_Crypto_00082]

[SWS_Crypto_00083]

[SWS_Crypto_00140]

[SWS_Crypto_00138]

[SWS_Crypto_00085]

[SWS_Crypto_00086]

[SWS_Crypto_00087]

[SWS_Crypto_00088]

[SWS_Crypto_00089]

[SWS_Crypto_00090]

[SWS_Crypto_00093]

[SWS_Crypto_00149]

[SWS_Crypto_00150]

[SWS_Crypto_00151]

[SWS_Crypto_00152]

[SWS_Crypto_00153]

[SWS_Crypto_00156]

[SWS_Crypto_00157]

[SWS_Crypto_00158]

[SWS_Crypto_00161]

[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.4 Specification Item SWS_Crylf_00017

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_GetVersionInfo shall **raise the error report** CRYIF_E_PARAM_POINTER to the **DET** if the parameter versioninfo is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are

the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to

SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength =

ciphertextLength," with
 "job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"
 [SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
 rename "state" to "jobState".
 [SWS_Csm_01026]: replace "associatedDataLength" with "associatedDataLength"
 [SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."
 [SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."
 [SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."
 [SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."
 [SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."
 [SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"
 –Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"
 –Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:
 replace "default error" detection with "development error detection" in requirement:
 [SWS_CryIf_00016]
 [SWS_CryIf_00017]
 [SWS_CryIf_00027]
 [SWS_CryIf_00028]
 [SWS_CryIf_00029]
 [SWS_CryIf_00129]
 [SWS_CryIf_00130]

[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]

[SWS_CryIf_00126]
[SWS_CryIf_00127]
[SWS_CryIf_00107]
[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]

[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.5 Specification Item SWS_CryIf_00027

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_ProcessJob shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGener-

ateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement. "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with

CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to

encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]

[SWS_CryIf_00099]
[SWS_CryIf_00123]
[SWS_CryIf_00124]
[SWS_CryIf_00125]
[SWS_CryIf_00126]
[SWS_CryIf_00127]
[SWS_CryIf_00107]
[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]

[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.6 Specification Item SWS_CryIf_00028

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_ProcessJob shall **raise the error report** CRYIF_E_PARAM_HANDLE to the **DET** and return E_NOT_OK if the parameter channelId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082]

Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]
[SWS_Crylf_00017]
[SWS_Crylf_00027]
[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]

[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]

[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer
—Last change on issue 76932 comment 2—

BW-C-Level:

Application	Specification	Bus
1	1	1

1.7 Specification Item SWS_CryIf_00029

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_ProcessJob shall **raise the error report** CRYIF_E_PARAM_POINTER **to the DET** and return E_NOT_OK if the parameter job is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMac-GenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]

[SWS_Crylf_00071]

[SWS_Crylf_00073]

[SWS_Crylf_00074]

[SWS_Crylf_00076]

[SWS_Crylf_00077]

[SWS_Crylf_00122]

[SWS_Crylf_00122]

[SWS_Crylf_00082]

[SWS_Crylf_00083]

[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]

[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.8 Specification Item SWS_CryIf_00049

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyElementSet shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength,

secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]

[SWS_Crylf_00071]

[SWS_Crylf_00073]

[SWS_Crylf_00074]

[SWS_Crylf_00076]

[SWS_Crylf_00077]

[SWS_Crylf_00122]

[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]

[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]

[SWS_Crypto_00173]

[SWS_Crypto_00174]

[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.9 Specification Item SWS_CryIf_00050

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyElementSet shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename

Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored."

On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"
–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]
[SWS_CryIf_00017]
[SWS_CryIf_00027]
[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]
[SWS_CryIf_00131]
[SWS_CryIf_00049]
[SWS_CryIf_00050]
[SWS_CryIf_00052]
[SWS_CryIf_00053]
[SWS_CryIf_00056]
[SWS_CryIf_00057]
[SWS_CryIf_00059]
[SWS_CryIf_00060]
[SWS_CryIf_00062]
[SWS_CryIf_00063]
[SWS_CryIf_00064]
[SWS_CryIf_00110]
[SWS_CryIf_00111]
[SWS_CryIf_00112]
[SWS_CryIf_00116]
[SWS_CryIf_00117]
[SWS_CryIf_00118]
[SWS_CryIf_00068]
[SWS_CryIf_00069]
[SWS_CryIf_00070]
[SWS_CryIf_00071]
[SWS_CryIf_00073]
[SWS_CryIf_00074]

[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]

[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]

[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.10 Specification Item SWS_CryIf_00052

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyElementSet shall **raise the error report** CRYIF_E_PARAM_POINTER to the **DET** and return E_NOT_OK if the parameter keyPtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist

anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element

'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCoun-

terRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]

[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]

[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.11 Specification Item SWS_CryIf_00053

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the Crypto Driver is enabled: The function CryIf_KeyElementSet shall **raise the error report** CRYIF_E_PARAM_VALUE **to the DET** and return E_NOT_OK if keyLength is zero.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into

the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = veri-

fyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the

key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]
[SWS_CryIf_00017]
[SWS_CryIf_00027]
[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]
[SWS_CryIf_00131]
[SWS_CryIf_00049]
[SWS_CryIf_00050]
[SWS_CryIf_00052]
[SWS_CryIf_00053]
[SWS_CryIf_00056]
[SWS_CryIf_00057]
[SWS_CryIf_00059]
[SWS_CryIf_00060]
[SWS_CryIf_00062]
[SWS_CryIf_00063]
[SWS_CryIf_00064]
[SWS_CryIf_00110]
[SWS_CryIf_00111]
[SWS_CryIf_00112]
[SWS_CryIf_00116]
[SWS_CryIf_00117]

[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]

[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]

[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

—Last change on issue 76932 comment 2—

BW-C-Level:

Application	Specification	Bus
1	1	1

1.12 Specification Item SWS_CryIf_00056

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeySetValid shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with

CryIf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamilyi -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_CryIf_00062]

[SWS_CryIf_00063]

[SWS_CryIf_00064]

[SWS_CryIf_00110]

[SWS_CryIf_00111]

[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]

[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]

[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.13 Specification Item SWS_CryIf_00057

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeySetValid shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement. "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, ter-

tiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: CryIf_KeyElementCopy() shall be replaced with CryIf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the

associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_CryIf_00062]

[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]

[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]

[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.14 Specification Item SWS_CryIf_00059

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyElementGet shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"
[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"
[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"
[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."
[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."
[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."
[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."
[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."
[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.
[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED
[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)
[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)
[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corre-

sponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]

[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.15 Specification Item SWS_CryIf_00060

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyElementGet shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text

according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".

rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]

[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]

[SWS_Crypto_00057]

[SWS_Crypto_00058]

[SWS_Crypto_00059]

[SWS_Crypto_00064]

[SWS_Crypto_00067]

[SWS_Crypto_00070]

[SWS_Crypto_00142]

[SWS_Crypto_00136]

[SWS_Crypto_00137]

[SWS_Crypto_00141]

[SWS_Crypto_00123]

[SWS_Crypto_00124]

[SWS_Crypto_00125]

[SWS_Crypto_00075]

[SWS_Crypto_00076]

[SWS_Crypto_00077]

[SWS_Crypto_00078]

[SWS_Crypto_00079]

[SWS_Crypto_00082]

[SWS_Crypto_00083]

[SWS_Crypto_00140]

[SWS_Crypto_00138]

[SWS_Crypto_00085]

[SWS_Crypto_00086]

[SWS_Crypto_00087]

[SWS_Crypto_00088]

[SWS_Crypto_00089]

[SWS_Crypto_00090]

[SWS_Crypto_00093]

[SWS_Crypto_00149]

[SWS_Crypto_00150]

[SWS_Crypto_00151]

[SWS_Crypto_00152]

[SWS_Crypto_00153]

[SWS_Crypto_00156]

[SWS_Crypto_00157]

[SWS_Crypto_00158]

[SWS_Crypto_00161]

[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.16 Specification Item SWS_CryIf_00062

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyElementGet shall **raise the error report** CRYIF_E_PARAM_POINTER to the **DET** and return E_NOT_OK if the parameter resultPtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are

the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to

SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength =

ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"
[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".
[SWS_Csm_01026]: replace "associatedDataLength" with "associatedDataLength"
[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."
[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."
[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."
[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."
[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."
[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"
–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"
–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:
replace "default error" detection with "development error detection" in requirement:
[SWS_CryIf_00016]
[SWS_CryIf_00017]
[SWS_CryIf_00027]
[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]

[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]

[SWS_CryIf_00126]
[SWS_CryIf_00127]
[SWS_CryIf_00107]
[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]

[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.17 Specification Item SWS_CryIf_00063

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyElementGet shall **raise the error report** CRYIF_E_PARAM_POINTER **to the DET** and return E_NOT_OK if the parameter resultLengthPtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGener-

ateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement. "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with

CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to

encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]

[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]

[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected
development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.18 Specification Item SWS_CryIf_00064

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyElementGet shall **raise the error report** CRYIF_E_PARAM_VALUE to the **DET** and return E_NOT_OK if the value, which is pointed by resultLengthPtr, is zero.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082]

Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]
[SWS_Crylf_00017]
[SWS_Crylf_00027]
[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]

[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]

[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer
—Last change on issue 76932 comment 2—

BW-C-Level:

Application	Specification	Bus
1	1	1

1.19 Specification Item SWS_CryIf_00068

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_RandomSeed shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMac-GenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]

[SWS_Crylf_00071]

[SWS_Crylf_00073]

[SWS_Crylf_00074]

[SWS_Crylf_00076]

[SWS_Crylf_00077]

[SWS_Crylf_00122]

[SWS_Crylf_00122]

[SWS_Crylf_00082]

[SWS_Crylf_00083]

[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]

[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.20 Specification Item SWS_CryIf_00069

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_RandomSeed shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength,

secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]

[SWS_Crylf_00071]

[SWS_Crylf_00073]

[SWS_Crylf_00074]

[SWS_Crylf_00076]

[SWS_Crylf_00077]

[SWS_Crylf_00122]

[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]

[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]

[SWS_Crypto_00173]

[SWS_Crypto_00174]

[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.21 Specification Item SWS_CryIf_00070

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_RandomSeed shall **raise the error report** CRYIF_E_PARAM_POINTER **to the DET** and return E_NOT_OK if the parameter seedPtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename

Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored."

On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"
–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]
[SWS_CryIf_00017]
[SWS_CryIf_00027]
[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]
[SWS_CryIf_00131]
[SWS_CryIf_00049]
[SWS_CryIf_00050]
[SWS_CryIf_00052]
[SWS_CryIf_00053]
[SWS_CryIf_00056]
[SWS_CryIf_00057]
[SWS_CryIf_00059]
[SWS_CryIf_00060]
[SWS_CryIf_00062]
[SWS_CryIf_00063]
[SWS_CryIf_00064]
[SWS_CryIf_00110]
[SWS_CryIf_00111]
[SWS_CryIf_00112]
[SWS_CryIf_00116]
[SWS_CryIf_00117]
[SWS_CryIf_00118]
[SWS_CryIf_00068]
[SWS_CryIf_00069]
[SWS_CryIf_00070]
[SWS_CryIf_00071]
[SWS_CryIf_00073]
[SWS_CryIf_00074]

[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]

[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]

[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.22 Specification Item SWS_CryIf_00071

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_RandomSeed shall **raise the error report** CRYIF_E_PARAM_VALUE to the **DET** and return E_NOT_OK if seedLength is zero.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist

anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element

'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service"

terRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]

[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]

[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.23 Specification Item SWS_CryIf_00073

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyGenerate shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into

the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = veri-

fyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the

key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]
[SWS_CryIf_00017]
[SWS_CryIf_00027]
[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]
[SWS_CryIf_00131]
[SWS_CryIf_00049]
[SWS_CryIf_00050]
[SWS_CryIf_00052]
[SWS_CryIf_00053]
[SWS_CryIf_00056]
[SWS_CryIf_00057]
[SWS_CryIf_00059]
[SWS_CryIf_00060]
[SWS_CryIf_00062]
[SWS_CryIf_00063]
[SWS_CryIf_00064]
[SWS_CryIf_00110]
[SWS_CryIf_00111]
[SWS_CryIf_00112]
[SWS_CryIf_00116]
[SWS_CryIf_00117]

[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]

[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]

[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.24 Specification Item SWS_CryIf_00074

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyGenerate shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with

CryIf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamilyi -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_CryIf_00062]

[SWS_CryIf_00063]

[SWS_CryIf_00064]

[SWS_CryIf_00110]

[SWS_CryIf_00111]

[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]

[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]

[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.25 Specification Item SWS_CryIf_00076

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyDerive shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement. "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00000]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00000]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00000]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, ter-

tiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the

associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_CryIf_00062]

[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]

[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]

[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.26 Specification Item SWS_CryIf_00077

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyDerive shall **raise the error report** CRYIF_E_PARAM_HANDLE to the **DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"
[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"
[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"
[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."
[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."
[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."
[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."
[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."
[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.
[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED
[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)
[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)
[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corre-

sponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]

[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.27 Specification Item SWS_CryIf_00082

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcPubVal shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text

according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".

rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]

[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]

[SWS_Crypto_00057]

[SWS_Crypto_00058]

[SWS_Crypto_00059]

[SWS_Crypto_00064]

[SWS_Crypto_00067]

[SWS_Crypto_00070]

[SWS_Crypto_00142]

[SWS_Crypto_00136]

[SWS_Crypto_00137]

[SWS_Crypto_00141]

[SWS_Crypto_00123]

[SWS_Crypto_00124]

[SWS_Crypto_00125]

[SWS_Crypto_00075]

[SWS_Crypto_00076]

[SWS_Crypto_00077]

[SWS_Crypto_00078]

[SWS_Crypto_00079]

[SWS_Crypto_00082]

[SWS_Crypto_00083]

[SWS_Crypto_00140]

[SWS_Crypto_00138]

[SWS_Crypto_00085]

[SWS_Crypto_00086]

[SWS_Crypto_00087]

[SWS_Crypto_00088]

[SWS_Crypto_00089]

[SWS_Crypto_00090]

[SWS_Crypto_00093]

[SWS_Crypto_00149]

[SWS_Crypto_00150]

[SWS_Crypto_00151]

[SWS_Crypto_00152]

[SWS_Crypto_00153]

[SWS_Crypto_00156]

[SWS_Crypto_00157]

[SWS_Crypto_00158]

[SWS_Crypto_00161]

[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.28 Specification Item SWS_Crylf_00083

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcPubVal shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are

the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to

SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength =

ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"
[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".
[SWS_Csm_01026]: replace "associatedDataLength" with "associatedDataLength"
[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."
[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."
[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."
[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."
[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."
[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"
–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"
–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:
replace "default error" detection with "development error detection" in requirement:
[SWS_CryIf_00016]
[SWS_CryIf_00017]
[SWS_CryIf_00027]
[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]

[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]

[SWS_CryIf_00126]
[SWS_CryIf_00127]
[SWS_CryIf_00107]
[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]

[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.29 Specification Item SWS_CryIf_00084

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcPubVal shall **raise the error report** CRYIF_E_PARAM_POINTER **to the DET** and return E_NOT_OK if the parameter publicValuePtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGener-

ateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement. "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with

CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to

encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]
[SWS_CryIf_00131]
[SWS_CryIf_00049]
[SWS_CryIf_00050]
[SWS_CryIf_00052]
[SWS_CryIf_00053]
[SWS_CryIf_00056]
[SWS_CryIf_00057]
[SWS_CryIf_00059]
[SWS_CryIf_00060]
[SWS_CryIf_00062]
[SWS_CryIf_00063]
[SWS_CryIf_00064]
[SWS_CryIf_00110]
[SWS_CryIf_00111]
[SWS_CryIf_00112]
[SWS_CryIf_00116]
[SWS_CryIf_00117]
[SWS_CryIf_00118]
[SWS_CryIf_00068]
[SWS_CryIf_00069]
[SWS_CryIf_00070]
[SWS_CryIf_00071]
[SWS_CryIf_00073]
[SWS_CryIf_00074]
[SWS_CryIf_00076]
[SWS_CryIf_00077]
[SWS_CryIf_00122]
[SWS_CryIf_00122]
[SWS_CryIf_00082]
[SWS_CryIf_00083]
[SWS_CryIf_00084]
[SWS_CryIf_00085]
[SWS_CryIf_00086]
[SWS_CryIf_00090]
[SWS_CryIf_00091]
[SWS_CryIf_00092]
[SWS_CryIf_00093]
[SWS_CryIf_00094]
[SWS_CryIf_00098]

[SWS_CryIf_00099]
[SWS_CryIf_00123]
[SWS_CryIf_00124]
[SWS_CryIf_00125]
[SWS_CryIf_00126]
[SWS_CryIf_00127]
[SWS_CryIf_00107]
[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]

[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected
development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.30 Specification Item SWS_CryIf_00085

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcPubVal shall **raise the error report** CRYIF_E_PARAM_POINTER to the **DET** and return E_NOT_OK if the parameter pubValueLengthPtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082]

Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]
[SWS_Crylf_00017]
[SWS_Crylf_00027]
[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]

[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]

[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer
—Last change on issue 76932 comment 2—

BW-C-Level:

Application	Specification	Bus
1	1	1

1.31 Specification Item SWS_CryIf_00086

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcPubVal shall **raise the error report** CRYIF_E_PARAM_VALUE **to the DET** and return E_NOT_OK if the value, which is pointed by pubValueLengthPtr, is zero.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMac-GenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]
[SWS_Crylf_00017]
[SWS_Crylf_00027]
[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]

[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]

[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.32 Specification Item SWS_CryIf_00090

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcSecret shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength,

secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]

[SWS_Crylf_00071]

[SWS_Crylf_00073]

[SWS_Crylf_00074]

[SWS_Crylf_00076]

[SWS_Crylf_00077]

[SWS_Crylf_00122]

[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]

[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]

[SWS_Crypto_00173]

[SWS_Crypto_00174]

[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.33 Specification Item SWS_CryIf_00091

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcSecret shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename

Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored."

On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"
–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]
[SWS_CryIf_00017]
[SWS_CryIf_00027]
[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]
[SWS_CryIf_00131]
[SWS_CryIf_00049]
[SWS_CryIf_00050]
[SWS_CryIf_00052]
[SWS_CryIf_00053]
[SWS_CryIf_00056]
[SWS_CryIf_00057]
[SWS_CryIf_00059]
[SWS_CryIf_00060]
[SWS_CryIf_00062]
[SWS_CryIf_00063]
[SWS_CryIf_00064]
[SWS_CryIf_00110]
[SWS_CryIf_00111]
[SWS_CryIf_00112]
[SWS_CryIf_00116]
[SWS_CryIf_00117]
[SWS_CryIf_00118]
[SWS_CryIf_00068]
[SWS_CryIf_00069]
[SWS_CryIf_00070]
[SWS_CryIf_00071]
[SWS_CryIf_00073]
[SWS_CryIf_00074]

[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]

[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]

[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.34 Specification Item SWS_CryIf_00092

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcSecret shall **raise the error report** CRYIF_E_PARAM_POINTER to the **DET** and return E_NOT_OK if the parameter partnerPublicValuePtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist

anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element

'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service"

terRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]

[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]

[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.35 Specification Item SWS_CryIf_00093

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcSecret shall **raise the error report** CRYIF_E_PARAM_POINTER **to the DET** and return E_NOT_OK if the parameter partnerPubValueLengthPtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceMan-

ager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]

[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]

[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.36 Specification Item SWS_CryIf_00094

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyExchangeCalcSecret shall **raise the error CRYPTOreport CRYIF_E_PARAM_VALUE to the DET** and return E_NOT_OK if partnerPubValue Length is zero.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function,

this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_CryIf_00062]

[SWS_CryIf_00063]

[SWS_CryIf_00064]

[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]

[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]

[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.37 Specification Item SWS_CryIf_00098

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_CertificateParse shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOut-

put". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]

[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]

[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.38 Specification Item SWS_CryIf_00099

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_CertificateParse shall **raise the error report** CRYIF_E_PARAM_HANDLE to the **DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"
[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"
[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"
[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."
[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."
[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."
[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."
[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."
[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.
[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED
[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)
[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)
[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corre-

sponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]

[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.39 Specification Item SWS_CryIf_00107

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function `CryIf_CallbackNotification` shall **raise the error report** `CRYIF_E_UNINIT` **to the DET** if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: `CRYPTO_E_KEY_EXTRACT_DENIED` does not exist anymore. Replace error code with `CRYPTO_E_KEY_READ_FAIL`.

[SWS_Crypto_91005]: `Crypto_KeyValidSet()` shall be named analogously to `Csm_KeySetValid()` and `CryIf_KeySetValid()`. Therefore, rename `Crypto_KeyValidSet()` to `Crypto_KeySetValid()`.

[SWS_Crypto_00071]: In table: `inputLengthPtr`, `secondaryInputLengthPtr`, `tertiaryInputLengthPtr` are no pointer anymore. rename them to `inputLength`, `secondaryInputLength`, `tertiaryInputLength`

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: `Csm_KeyCopy()` shall call `CryIf_KeyCopy()` not `CryIf_KeyElementCopy()`.

[SWS_Csm_01080]: `Csm_AsymPrivateKeyType` is not up-to-date. It should be modified like [SWS_Csm_00076] `Csm_AsymPublicKeyType` or [SWS_Csm_01082] `Csm_SymKeyType`.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: `CsmMacGenerateAlgorithmFamiliy` -> `CsmMacGenerateAlgorithmFamily`

[ECUC_Csm_00049]: `CsmMacVerifyAlgorithmMode` missing. (see analogues `CsmMacGenerateAlgorithmMode` [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: `plaintextLength` description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text

according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".

rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]

[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]

[SWS_Crypto_00057]

[SWS_Crypto_00058]

[SWS_Crypto_00059]

[SWS_Crypto_00064]

[SWS_Crypto_00067]

[SWS_Crypto_00070]

[SWS_Crypto_00142]

[SWS_Crypto_00136]

[SWS_Crypto_00137]

[SWS_Crypto_00141]

[SWS_Crypto_00123]

[SWS_Crypto_00124]

[SWS_Crypto_00125]

[SWS_Crypto_00075]

[SWS_Crypto_00076]

[SWS_Crypto_00077]

[SWS_Crypto_00078]

[SWS_Crypto_00079]

[SWS_Crypto_00082]

[SWS_Crypto_00083]

[SWS_Crypto_00140]

[SWS_Crypto_00138]

[SWS_Crypto_00085]

[SWS_Crypto_00086]

[SWS_Crypto_00087]

[SWS_Crypto_00088]

[SWS_Crypto_00089]

[SWS_Crypto_00090]

[SWS_Crypto_00093]

[SWS_Crypto_00149]

[SWS_Crypto_00150]

[SWS_Crypto_00151]

[SWS_Crypto_00152]

[SWS_Crypto_00153]

[SWS_Crypto_00156]

[SWS_Crypto_00157]

[SWS_Crypto_00158]

[SWS_Crypto_00161]

[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.40 Specification Item SWS_Crylf_00108

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_CallbackNotification shall **raise the error report** CRYIF_E_PARAM_POINTER **to the DET** if the parameter job is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are

the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to

SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength =

ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"
[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".
[SWS_Csm_01026]: replace "associatedDataLength" with "associatedDataLength"
[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."
[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."
[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."
[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."
[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."
[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"
–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"
–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:
replace "default error" detection with "development error detection" in requirement:
[SWS_CryIf_00016]
[SWS_CryIf_00017]
[SWS_CryIf_00027]
[SWS_CryIf_00028]
[SWS_CryIf_00029]
[SWS_CryIf_00129]
[SWS_CryIf_00130]

[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]

[SWS_CryIf_00126]
[SWS_CryIf_00127]
[SWS_CryIf_00107]
[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]

[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.41 Specification Item SWS_CryIf_00110

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_KeyElementCopy shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGener-

ateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement. "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with

CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to

encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]

[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]

[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected
development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.42 Specification Item SWS_CryIf_00111

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_KeyElementCopy shall **raise the error report** CRYIF_E_PARAM_HANDLE to the **DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082]

Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]
[SWS_Crylf_00017]
[SWS_Crylf_00027]
[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]

[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]

[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer
—Last change on issue 76932 comment 2—

BW-C-Level:

Application	Specification	Bus
1	1	1

1.43 Specification Item SWS_CryIf_00112

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_KeyElementCopy shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter targetCryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMac-GenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]
[SWS_Crylf_00017]
[SWS_Crylf_00027]
[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]

[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]

[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.44 Specification Item SWS_CryIf_00115

Trace References:

SRS_CryptoStack_00034

Content:

If a key element of cryIfKeyId is not available in targetCryIfKeyId, the key element shall not be copied and no error code shall be returned.

If the source element size does not match the target key elements size, CryIf_KeyElement Copy() shall **raise the error report** CRYIF_E_KEY_SIZE_MISMATCH **to the DET** and return E_NOT_OK.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename

Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored."

On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

1.45 Specification Item SWS_CryIf_00116

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_KeyCopy shall **raise the error report** CRYIF_E_UNINIT to the **DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082]

Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]
[SWS_Crylf_00017]
[SWS_Crylf_00027]
[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]

[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]

[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer
—Last change on issue 76932 comment 2—

BW-C-Level:

Application	Specification	Bus
1	1	1

1.46 Specification Item SWS_CryIf_00117

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_KeyCopy shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMac-GenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]
[SWS_Crylf_00017]
[SWS_Crylf_00027]
[SWS_Crylf_00028]
[SWS_Crylf_00029]
[SWS_Crylf_00129]
[SWS_Crylf_00130]
[SWS_Crylf_00131]
[SWS_Crylf_00049]
[SWS_Crylf_00050]
[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]

[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]

[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.47 Specification Item SWS_CryIf_00118

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_KeyCopy shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the parameter targetCryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength,

secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_CryIf_00062]

[SWS_CryIf_00063]

[SWS_CryIf_00064]

[SWS_CryIf_00110]

[SWS_CryIf_00111]

[SWS_CryIf_00112]

[SWS_CryIf_00116]

[SWS_CryIf_00117]

[SWS_CryIf_00118]

[SWS_CryIf_00068]

[SWS_CryIf_00069]

[SWS_CryIf_00070]

[SWS_CryIf_00071]

[SWS_CryIf_00073]

[SWS_CryIf_00074]

[SWS_CryIf_00076]

[SWS_CryIf_00077]

[SWS_CryIf_00122]

[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]

[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]

[SWS_Crypto_00173]

[SWS_Crypto_00174]

[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.48 Specification Item SWS_CryIf_00121

Trace References:

SRS_CryptoStack_00034

Content:

If a key element of cryIfKeyId is not available in targetCryIfKeyId, the key element shall not be copied and no error code shall be returned.

If the source element size does not match the target key elements size, CryIf_Key Copy() shall **raise the error report** CRYIF_E_KEY_SIZE_MISMATCH **to the DET** and return E_NOT_OK.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist

anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element

'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service"

terRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

1.49 Specification Item SWS_CryIf_00122

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_KeyDerive shall **raise the error report** CRYIF_E_PARAM_HANDLE to the **DET** and return E_NOT_OK if the parameter targetCryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMac-GenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]

[SWS_Crylf_00071]

[SWS_Crylf_00073]

[SWS_Crylf_00074]

[SWS_Crylf_00076]

[SWS_Crylf_00077]

[SWS_Crylf_00122]

[SWS_Crylf_00122]

[SWS_Crylf_00082]

[SWS_Crylf_00083]

[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]

[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.50 Specification Item SWS_CryIf_00123

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_CertificateVerify shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength,

secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]

[SWS_Crylf_00071]

[SWS_Crylf_00073]

[SWS_Crylf_00074]

[SWS_Crylf_00076]

[SWS_Crylf_00077]

[SWS_Crylf_00122]

[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]

[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]

[SWS_Crypto_00173]

[SWS_Crypto_00174]

[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.51 Specification Item SWS_CryIf_00124

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_CertificateVerify shall **raise the error report** CRYIF_E_PARAM_HANDLE to the **DET** and return E_NOT_OK if the parameter cryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename

Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored."

On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_CryIf_00062]

[SWS_CryIf_00063]

[SWS_CryIf_00064]

[SWS_CryIf_00110]

[SWS_CryIf_00111]

[SWS_CryIf_00112]

[SWS_CryIf_00116]

[SWS_CryIf_00117]

[SWS_CryIf_00118]

[SWS_CryIf_00068]

[SWS_CryIf_00069]

[SWS_CryIf_00070]

[SWS_CryIf_00071]

[SWS_CryIf_00073]

[SWS_CryIf_00074]

[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]

[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]

[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.52 Specification Item SWS_CryIf_00125

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_CertificateVerify shall **raise the error report** CRYIF_E_PARAM_HANDLE to the **DET** and return E_NOT_OK if the parameter validateCryIfKeyId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist

anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element

'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCoun-

terRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]

[SWS_Crylf_00118]

[SWS_Crylf_00068]

[SWS_Crylf_00069]

[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]

[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]

[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.53 Specification Item SWS_CryIf_00126

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function Cry If_CertificateVerify shall **raise the error report** CRYIF_E_PARAM_HANDLE **to the DET** and return E_NOT_OK if the keys identified by validateCryIfKeyId and cryIfKeyId are not located in the same Crypto Driver.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceMan-

ager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_Crylf:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crylf_00016]

[SWS_Crylf_00017]

[SWS_Crylf_00027]

[SWS_Crylf_00028]

[SWS_Crylf_00029]

[SWS_Crylf_00129]

[SWS_Crylf_00130]

[SWS_Crylf_00131]

[SWS_Crylf_00049]

[SWS_Crylf_00050]

[SWS_Crylf_00052]

[SWS_Crylf_00053]

[SWS_Crylf_00056]

[SWS_Crylf_00057]

[SWS_Crylf_00059]

[SWS_Crylf_00060]

[SWS_Crylf_00062]

[SWS_Crylf_00063]

[SWS_Crylf_00064]

[SWS_Crylf_00110]

[SWS_Crylf_00111]

[SWS_Crylf_00112]

[SWS_Crylf_00116]

[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]

[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]

[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.54 Specification Item SWS_CryIf_00127

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF module is enabled: The function CryIf_CertificateVerify shall **raise the error report** CRYIF_E_PARAM_POINTER to the **DET** and return E_NOT_OK if the parameter verifyPtr is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copy paste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copy paste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function,

this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_CryIf_00062]

[SWS_CryIf_00063]

[SWS_CryIf_00064]

[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]

[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]

[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.55 Specification Item SWS_CryIf_00129

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_Cancel Job shall **raise the error report** CRYIF_E_UNINIT **to the DET** and return E_NOT_OK if the module is not yet initialized.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and Crylf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOut-

put". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00071]: rename `inputLengthPtr`, `secondaryInputLengthPtr`, `tertiaryInputLengthPtr` to `inputLength`, `secondaryInputLength`, `tertiaryInputLength`

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: `Crylf_KeyElementCopy()` shall be replaced with `Crylf_KeyCopy()`.

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: `Csm_AsymPrivateKeyType`

Kind: Structure

Elements:

length: `uint32`: This element contains the length in bytes of the key stored in element 'data'

data: `Csm_AsymPrivateKeyArrayType`: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: `CsmMacGenerateAlgorithmFamiiliy` -> `CsmMacGenerateAlgorithmFamily`

[ECUC_Csm_00049]: add `CsmMacVerifyAlgorithmMode` (see analogues `CsmMacGenerateAlgorithmMode` [ECUC_Csm_00189])

[ECUC_Csm_00049]: add `CsmMacVerifyAlgorithmModeCustom` (see analogues `CsmMacGenerateAlgorithmModeCustom` [ECUC_Csm_00189])

[ECUC_Csm_00049]: add `CsmMacVerifyAlgorithmKeyLength` (see analogues `CsmMacGenerateAlgorithmKeyLength` [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "`associatedDataLengthPtr`" with "`associatedDataLength`"

[SWS_Csm_01025]: Replace line "`job->jobPrimitiveInputOutput.outputLength = ciphertextLength,`" with

"`job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,`"

[SWS_Csm_01013]: rename "`PrimitiveInputOutput`" to "`jobPrimitiveInputOutput`".
rename "`state`" to "`jobState`".

[SWS_Csm_01026]: replace "`associatatedDataLength`" with "`associatedDataLength`"

[SWS_Csm_01027]: add line: "`job->jobPrimitiveInputOutput.verifyPtr = verifyPtr.`"

[SWS_Csm_00992]: replace "mode: The `Crypto_JobInfoType` job with the corresponding `jobId` shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

–Last change on issue 76932 comment 2–

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_CryIf_00059]

[SWS_CryIf_00060]

[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]

[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]

[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.56 Specification Item SWS_CryIf_00130

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_Cancel Job shall **raise the error report** CRYIF_E_PARAM_HANDLE to the **DET** and return E_NOT_OK if the parameter channelId is out of range.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"
[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"
[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"
[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."
[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."
[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."
[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."
[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."
[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:
[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.
[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED
[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)
[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)
[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.
[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corre-

sponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_CryIf_00052]

[SWS_CryIf_00053]

[SWS_CryIf_00056]

[SWS_CryIf_00057]

[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]
[SWS_Crylf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]
[SWS_Crypto_00057]
[SWS_Crypto_00058]
[SWS_Crypto_00059]
[SWS_Crypto_00064]
[SWS_Crypto_00067]
[SWS_Crypto_00070]
[SWS_Crypto_00142]
[SWS_Crypto_00136]
[SWS_Crypto_00137]
[SWS_Crypto_00141]
[SWS_Crypto_00123]
[SWS_Crypto_00124]
[SWS_Crypto_00125]
[SWS_Crypto_00075]
[SWS_Crypto_00076]
[SWS_Crypto_00077]
[SWS_Crypto_00078]
[SWS_Crypto_00079]
[SWS_Crypto_00082]
[SWS_Crypto_00083]
[SWS_Crypto_00140]
[SWS_Crypto_00138]
[SWS_Crypto_00085]
[SWS_Crypto_00086]
[SWS_Crypto_00087]
[SWS_Crypto_00088]
[SWS_Crypto_00089]
[SWS_Crypto_00090]
[SWS_Crypto_00093]
[SWS_Crypto_00149]
[SWS_Crypto_00150]
[SWS_Crypto_00151]
[SWS_Crypto_00152]
[SWS_Crypto_00153]
[SWS_Crypto_00156]
[SWS_Crypto_00157]
[SWS_Crypto_00158]
[SWS_Crypto_00161]
[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]

[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer
→Default Error Tracer
–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.57 Specification Item SWS_Crylf_00131

Trace References:

SRS_CryptoStack_00034

Content:

If **default development** error detection for the CRYIF is enabled: The function CryIf_Cancel Job shall **raise the error report** CRYIF_E_PARAM_POINTER to the **DET** and return E_NOT_OK if the parameter job is a null pointer.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call CryIf_KeyCopy() not CryIf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associatatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with
"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?
Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like
"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_CryIf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text

according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_00083]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".

rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

—Last change on issue 76783 comment 29—

BW-C-Level:

Application	Specification	Bus
4	3	1

- RfC #76932: default error detection -> development error detection

Problem description:

replace "default error detection" with "development error detection"

—Last change on issue 76932 comment 2—

Agreed solution:

SWS_CryIf:

replace "default error" detection with "development error detection" in requirement:

[SWS_CryIf_00016]

[SWS_CryIf_00017]

[SWS_CryIf_00027]

[SWS_CryIf_00028]

[SWS_CryIf_00029]

[SWS_CryIf_00129]

[SWS_CryIf_00130]

[SWS_CryIf_00131]

[SWS_CryIf_00049]

[SWS_CryIf_00050]

[SWS_Crylf_00052]
[SWS_Crylf_00053]
[SWS_Crylf_00056]
[SWS_Crylf_00057]
[SWS_Crylf_00059]
[SWS_Crylf_00060]
[SWS_Crylf_00062]
[SWS_Crylf_00063]
[SWS_Crylf_00064]
[SWS_Crylf_00110]
[SWS_Crylf_00111]
[SWS_Crylf_00112]
[SWS_Crylf_00116]
[SWS_Crylf_00117]
[SWS_Crylf_00118]
[SWS_Crylf_00068]
[SWS_Crylf_00069]
[SWS_Crylf_00070]
[SWS_Crylf_00071]
[SWS_Crylf_00073]
[SWS_Crylf_00074]
[SWS_Crylf_00076]
[SWS_Crylf_00077]
[SWS_Crylf_00122]
[SWS_Crylf_00122]
[SWS_Crylf_00082]
[SWS_Crylf_00083]
[SWS_Crylf_00084]
[SWS_Crylf_00085]
[SWS_Crylf_00086]
[SWS_Crylf_00090]
[SWS_Crylf_00091]
[SWS_Crylf_00092]
[SWS_Crylf_00093]
[SWS_Crylf_00094]
[SWS_Crylf_00098]
[SWS_Crylf_00099]
[SWS_Crylf_00123]
[SWS_Crylf_00124]
[SWS_Crylf_00125]
[SWS_Crylf_00126]
[SWS_Crylf_00127]
[SWS_Crylf_00107]

[SWS_CryIf_00108]

SWS_Crypto:

replace "default error" detection with "development error detection" in requirement:

[SWS_Crypto_00047]

[SWS_Crypto_00057]

[SWS_Crypto_00058]

[SWS_Crypto_00059]

[SWS_Crypto_00064]

[SWS_Crypto_00067]

[SWS_Crypto_00070]

[SWS_Crypto_00142]

[SWS_Crypto_00136]

[SWS_Crypto_00137]

[SWS_Crypto_00141]

[SWS_Crypto_00123]

[SWS_Crypto_00124]

[SWS_Crypto_00125]

[SWS_Crypto_00075]

[SWS_Crypto_00076]

[SWS_Crypto_00077]

[SWS_Crypto_00078]

[SWS_Crypto_00079]

[SWS_Crypto_00082]

[SWS_Crypto_00083]

[SWS_Crypto_00140]

[SWS_Crypto_00138]

[SWS_Crypto_00085]

[SWS_Crypto_00086]

[SWS_Crypto_00087]

[SWS_Crypto_00088]

[SWS_Crypto_00089]

[SWS_Crypto_00090]

[SWS_Crypto_00093]

[SWS_Crypto_00149]

[SWS_Crypto_00150]

[SWS_Crypto_00151]

[SWS_Crypto_00152]

[SWS_Crypto_00153]

[SWS_Crypto_00156]

[SWS_Crypto_00157]

[SWS_Crypto_00158]

[SWS_Crypto_00161]

[SWS_Crypto_00162]
[SWS_Crypto_00163]
[SWS_Crypto_00164]
[SWS_Crypto_00128]
[SWS_Crypto_00129]
[SWS_Crypto_00130]
[SWS_Crypto_00131]
[SWS_Crypto_00094]
[SWS_Crypto_00095]
[SWS_Crypto_00097]
[SWS_Crypto_00098]
[SWS_Crypto_00103]
[SWS_Crypto_00104]
[SWS_Crypto_00105]
[SWS_Crypto_00106]
[SWS_Crypto_00107]
[SWS_Crypto_00110]
[SWS_Crypto_00111]
[SWS_Crypto_00112]
[SWS_Crypto_00113]
[SWS_Crypto_00115]
[SWS_Crypto_00168]
[SWS_Crypto_00169]
[SWS_Crypto_00172]
[SWS_Crypto_00173]
[SWS_Crypto_00174]
[SWS_Crypto_00175]

SRS_Crypto:

[SRS_CryptoStack_00087] The CSM module shall report detected development errors to the Development Error Tracer

→Default Error Tracer

–Last change on issue 76932 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.58 Specification Item SWS_Crylf_91003

Trace References:

none

Content:

Service name:	CryIf_ProcessJobCryIf_ProcessJob	
Syntax:	Std_ReturnType CryIf_ProcessJob(uint32 channelId, Crypto_JobType* job)	
Service ID[hex]:	0x03	
Sync/Async:	Sync or Async, depends on the configuration	
Reentrancy:	Reentrant	
Parameters (in):	channelIdCryIf_ProcessJob.channelId	Holds the identifier of the crypto channel.
Parameters (inout):	jobCryIf_ProcessJob.job	Pointer to the configuration of the job. Contains structures with user and primitive relevant information.
Parameters (out):	None	
Return value:	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_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size. CRYIFCRYPTO_E_QUEUE_FULL: Request failed, the queue is full CRYIFCRYPTO_E_SMALL_BUFFER: The provided buffer is too small to store the result CRYPTO_E_JOB_CANCELED: The service request failed because the synchronous Job has been canceled.
Description:	This interface dispatches the received jobs to the configured crypto driver object.	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76636: Rollout of 'Runtime errors' for entire crypto stack documents

Problem description:

Crypto Stack documents are not in line with the RfC # 59085.

In SWS_secureOnboardCommunication

Example1: SECOC_E_CRYPTO_FAILURE in the is a development error, but should be a runtime error.

In SWS_CryptoServiceManager

Example2: CSM_E_SERVICE_NOT_STARTED is not referenced.

Example3: CSM_E_PARAM_HANDLE is not referenced in chapter 7.3. It is not clear development error or runtime error.

–Last change on issue 76636 comment 33–

Agreed solution:

CryptoInterface:

<https://bugzilla.autosar.org/attachment.cgi?id=4587>

CryptoServiceManager:

<https://bugzilla.autosar.org/attachment.cgi?id=4614>

CryptoDriver:

<https://bugzilla.autosar.org/attachment.cgi?id=4613>

SecureOnboardCommunication:

<https://bugzilla.autosar.org/attachment.cgi?id=4598>

–Last change on issue 76636 comment 41–

BW-C-Level:

Application	Specification	Bus
1	4	1

1.59 Specification Item SWS_CryIf_91015

Trace References:

none

Content:

Service name:	CryIf_KeyElementCopyCryIf_KeyElementCopy
Syntax:	Std_ReturnType CryIf_KeyElementCopy(uint32 cryIfKeyId, uint32 keyElementId, uint32 targetCryIfKeyId, uint32 targetKeyElementId)
Service ID[hex]:	0x0f
Sync/Async:	Synchronous
Reentrancy:	Reentrant, but not for the same cryIfKeyId

Parameters (in):	cryIfKeyIdCryIf_KeyElementCopy.cryIfKeyId	Holds the identifier of the key whose key element shall be the source element.
	keyElementIdCryIf_KeyElementCopy.keyElementId	Holds the identifier of the key element which shall be the source for the copy operation.
	targetCryIfKeyIdCryIf_KeyElementCopy.targetCryIfKeyId	Holds the identifier of the key whose key element shall be the destination element.
	targetKeyElementIdCryIf_KeyElementCopy.targetKeyElementId	Holds the identifier of the key element which shall be the destination for the copy operation.
Parameters (inout):	None	
Parameters (out):	None	
Return value:	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_AVAILABLE: Request failed, the requested key element is not available CRYPTO_E_KEY_EXTRACT_DENIED: Request failed, not allowed to extract key element CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element. CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible.
Description:	This function shall copy a key elements from one key to a target key.	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76783: Typo or copy/paste mistakes

Problem description:

Hello,

I found some other mistakes in the specification documents. Most of them are typos or copy/paste mistakes. As document owner of the CryptoServiceManager, I need a confirmation from someone else, before I can implement them into the document.

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: CRYPTO_E_KEY_EXTRACT_DENIED does not exist anymore. Replace error code with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crypto_91005]: Crypto_KeyValidSet() shall be named analogously to Csm_KeySetValid() and CryIf_KeySetValid(). Therefore, rename

Crypto_KeyValidSet() to Crypto_KeySetValid().

[SWS_Crypto_00071]: In table: inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr are no pointer anymore. rename them to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Csm_KeyCopy() shall call Crylf_KeyCopy() not Crylf_KeyElementCopy().

[SWS_Csm_01080]: Csm_AsymPrivateKeyType is not up-to-date. It should be modified like [SWS_Csm_00076] Csm_AsymPublicKeyType or [SWS_Csm_01082] Csm_SymKeyType.

SWS_Csm_00455

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: CsmMacVerifyAlgorithmMode missing. (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[SWS_Csm_00966]: CopyPaste mistake: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: plaintextLength description wrong. replace with "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: typo "associtatedDataLengthPtr" and it is no pointer. replace with: "associatedDataLength"

[SWS_Csm_01025]: typo, replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: typo: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput". Or is this rename intended?

Then every assignment of "jobPrimitiveInputOutput" has to be renamed to "primitiveInputOutput" like

"job->jobPrimitiveInputOutput.mode = mode," has to be modified to "job->primitiveInputOutput.mode = mode,"

[SWS_Csm_01026]: typo: replace "associtatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: missing line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: copypaste mistake: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: copypaste mistake: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored."

On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: description wrong. replace with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: description wrong, there is no IV. replace with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: description wrong, it is not decrement.
"CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

A proposed solution is added, too.

Agreed solution:

AUTOSAR_SWS_CryptoDriver:

[SWS_Crypto_00139]: Replace CRYPTO_E_KEY_EXTRACT_DENIED with CRYPTO_E_KEY_READ_FAIL.

[SWS_Crylf_91015]: Remove CRYPTO_E_KEY_EXTRACT_DENIED

[SWS_Crypto_91005]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add Crypto_KeySetValid as API (Description according to SWS_Crypto_91005)

[SWS_Crypto_00082]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_UNINIT DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00082)

[SWS_Crypto_00083]: Set Crypto_KeyValidSet obsolete.

[SWS_Crypto_xxx]: Add E_PARAM_HANDLE DET check SWS for Crypto_KeySetValid (Text according to SWS_Crypto_00083)

last sentence in 8.2.4.1.2: Rename Crypto_KeyValidSet to Crypto_KeySetValid

[SWS_Crypto_00071]: rename inputLengthPtr, secondaryInputLengthPtr, tertiaryInputLengthPtr to inputLength, secondaryInputLength, tertiaryInputLength

AUTOSAR_SWS_CryptoServiceManager:

[SWS_Csm_01035]: Crylf_KeyElementCopy() shall be replaced with Crylf_KeyCopy().

[SWS_Csm_01080]: replace with (see [SWS_Csm_00076]):

Name: Csm_AsymPrivateKeyType

Kind: Structure

Elements:

length: uint32: This element contains the length in bytes of the key stored in element 'data'

data: Csm_AsymPrivateKeyArrayType: This element contains the key data or a key handle.

Description: Structure for the private asymmetrical key.

Variation: –

[SWS_Csm_00455]: tag as obsolete

[ECUC_Csm_00188]: typo: CsmMacGenerateAlgorithmFamiliy -> CsmMacGenerateAlgorithmFamily

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmMode (see analogues CsmMacGenerateAlgorithmMode [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmModeCustom (see analogues CsmMacGenerateAlgorithmModeCustom [ECUC_Csm_00189])

[ECUC_Csm_00049]: add CsmMacVerifyAlgorithmKeyLength (see analogues CsmMacGenerateAlgorithmKeyLength [ECUC_Csm_00189])

[SWS_Csm_00966]: Delete: "Wrong return values - here are the correct ones:"

[SWS_Csm_01023]: Replace description with: "Contains the number of bytes to encrypt."

[SWS_Csm_01023]: Replace "associatedDataLengthPtr" with "associatedDataLength"

[SWS_Csm_01025]: Replace line "job->jobPrimitiveInputOutput.outputLength = ciphertextLength," with

"job->jobPrimitiveInputOutput.outputLengthPtr = ciphertextLengthPtr,"

[SWS_Csm_01013]: rename "PrimitiveInputOutput" to "jobPrimitiveInputOutput".
rename "state" to "jobState".

[SWS_Csm_01026]: replace "associatatedDataLength" with "associatedDataLength"

[SWS_Csm_01027]: add line: "job->jobPrimitiveInputOutput.verifyPtr = verifyPtr."

[SWS_Csm_00992]: replace "mode: The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:" with ""mode: Indicates which operation mode(s) to perform."

[SWS_Csm_00992]: replace "resultLengthPtr: Contains the number of bytes of the associated data." with ""resultLengthPtr: Holds a pointer to the memory location in which the output length in bytes of the signature is stored. On calling this function, this parameter shall contain the size of the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored."

[SWS_Csm_01543]: replace description with "Generate a random number and stores it in the memory location pointed by the result pointer."

[SWS_Csm_00168]: replace description with "This function is deprecated. Sets the key for symmetrical encryption."

[SWS_Csm_01031]: replace "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterDecrement Service" with "CRYPTO_SECCOUNTERREAD 0x0A SecureCounterRead Service"

–Last change on issue 76783 comment 29–

BW-C-Level:

Application	Specification	Bus
4	3	1