Document Title	SWS_CryptoServiceManager: 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_CryptoServiceManager

1.1 Specification Item ECUC_Csm_00015

Trace References:

none

Content:

Name	CsmKeyIdCsmKey.CsmKeyId		
Parent Container	CsmKey		
Description	Identifier of the CsmKey. The set of actually configured identifiers shall be consecutive and gapless.		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	1 0 .. 4294967295		
Default value	–		
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77049: [CRYPTO] CsmJob|Key|CallbackId configuration parameters

  Problem description:

  There are configuration parameters "CsmJob|Key|CallbackId".
  Why are these parameters specified or why are they configurable by the user?
  I think it would be more reasonable if these, only internal relevant 'values' will be auto-created by the AUTOSAR stack configuration and code generation tools, including symbolic names for this 'values' for the user.

  Especially because in my opinion it is only meaningful to number these Ids consecutively, starting from zero, incremented by one.
  Only in this way the Job, Key or Callback configurations are arrangeable in C arrays whose elements can be directly accessed (via the Id). This is the most memory and run-time optimal solution.

(=> cmp. "Specification of Crypto Service Manager", 4.0.3, section "11.4 Configuration of the Configuration IDs")

Agreed solution:

remove note in "10.2 Containers and Configuration Parameters"
"Note: The Ids in the configuration containers shall be consecutive, gapless and shall start from zero"

[ECUC_Csm_00119] CsmJobId,
- append to description: ". The set of actually configured identifiers shall be consecutive and gapless."

[ECUC_Csm_00015] CsmKeyId,
- append to description: ". The set of actually configured identifiers shall be consecutive and gapless."
- change Range to: 0 .. 4294967295

[ECUC_Csm_00111] CsmCallbackId,
- append to description: ". The set of actually configured identifiers shall be consecutive and gapless."
- change Range to: 0 .. 4294967295
–Last change on issue 77049 comment 7–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.2 Specification Item ECUC_Csm_00036

Trace References:

none

Content:

Container Name	CsmHashConfigCsmHashConfig
Description	Container for configuration of a CSM hash. The container name serves as a symbolic name for the identifier of a key configuration.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmHashAlgorithm~~Familiy~~ Family	ECUC_Csm_00038
CsmHashAlgorithmFamilyCustom	ECUC_Csm_00128
CsmHashAlgorithmMode	ECUC_Csm_00131
CsmHashAlgorithmModeCustom	ECUC_Csm_00132
CsmHashAlgorithmSecondaryFamily	ECUC_Csm_00181
CsmHashAlgorithmSecondaryFamilyCustom	ECUC_Csm_00129
CsmHashDataMaxLength	ECUC_Csm_00040
CsmHashProcessing	ECUC_Csm_00039
CsmHashResultLength	ECUC_Csm_00130

Included containers:

No Included Containers

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.3 Specification Item ECUC_Csm_00038

Trace References:

none

Content:

Name	CsmHashAlgorithmFamiliyFamilyCsmHashConfig.CsmHashAlgorithmFamiliy Family
Parent Container	CsmHashConfig
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.
Multiplicity	1
Type	EcucEnumerationParamDef

Range	CRYPTO_ALGOFAM_BLAKE_1_256	0x0F	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_BLAKE_1_256
	CRYPTO_ALGOFAM_BLAKE_1_512	0x10	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_BLAKE_1_512
	CRYPTO_ALGOFAM_BLAKE_2s_256	0x11	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_BLAKE_2s_256
	CRYPTO_ALGOFAM_BLAKE_2s_512	0x12	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_BLAKE_2s_512
	CRYPTO_ALGOFAM_CUSTOM	0xFF	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_CUSTOM
	CRYPTO_ALGOFAM_RIPEMD160	0x0E	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_RIPEMD160
	CRYPTO_ALGOFAM_SHA1	0x01	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA1
	CRYPTO_ALGOFAM_SHA2_224	0x02	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA2_224
	CRYPTO_ALGOFAM_SHA2_256	0x03	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA2_256
	CRYPTO_ALGOFAM_SHA2_384	0x04	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA2_384
	CRYPTO_ALGOFAM_SHA2_512	0x05	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA2_512
	CRYPTO_ALGOFAM_SHA2_512_224	0x06	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA2_512_224
	CRYPTO_ALGOFAM_SHA2_512_256	0x07	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA2_512_256
	CRYPTO_ALGOFAM_SHA3_224	0x08	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA3_224
	CRYPTO_ALGOFAM_SHA3_256	0x09	CsmHashConfig.CsmHashAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_SHA3_256
	CRYPTO_ALGOFAM_SHA3_384	0x0A	Csm

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

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035
  ECUC_Crypto_00037
  –Last change on issue 77711 comment 8–

  BW-C-Level:

Application	Specification	Bus
1	3	1

1.4 Specification Item ECUC_Csm_00041

Trace References:

none

Content:

Container Name	CsmMacGenerateConfigCsmMacGenerateConfig
Description	Container for configuration of a CSM mac generation interface. The container name serves as a symbolic name for the identifier of a MAC generation interface.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmMacGenerateAlgorithmFamiliy Family	ECUC_Csm_00188
CsmMacGenerateAlgorithmFamilyCustom	ECUC_Csm_00133
CsmMacGenerateAlgorithmKeyLength	ECUC_Csm_00044
CsmMacGenerateAlgorithmMode	ECUC_Csm_00189
CsmMacGenerateAlgorithmModeCustom	ECUC_Csm_00136
CsmMacGenerateAlgorithmSecondaryFamily	ECUC_Csm_00134
CsmMacGenerateAlgorithmSecondaryFamilyCustom	ECUC_Csm_00135
CsmMacGenerateDataMaxLength	ECUC_Csm_00137
CsmMacGenerateProcessing	ECUC_Csm_00046
CsmMacGenerateResultLength	ECUC_Csm_00138

Included containers:

No Included Containers

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.

There is an "i" before the "y" in "Family".

RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

Agreed solution:

Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
ECUC_Csm_00038
ECUC_Csm_00188
ECUC_Csm_00051
ECUC_Csm_00182
ECUC_Csm_00066
ECUC_Csm_00074
ECUC_Csm_00082
ECUC_Csm_00089
ECUC_Csm_00096
ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.5 Specification Item ECUC_Csm_00049

Trace References:

none

Content:

Container Name	CsmMacVerifyConfigCsmMacVerifyConfig
Description	Container for configuration of a CSM MAC verification interface. The container name serves as a symbolic name for the identifier of a MAC generation interface
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmMacVerifyAlgorithmFamiliy Family	ECUC_Csm_00051
CsmMacVerifyAlgorithmFamilyCustom	ECUC_Csm_00139
CsmMacVerifyAlgorithmKeyLength	ECUC_Csm_00193
CsmMacVerifyAlgorithmMode	ECUC_Csm_00195
CsmMacVerifyAlgorithmModeCustom	ECUC_Csm_00194
CsmMacVerifyAlgorithmSecondaryFamily	ECUC_Csm_00140
CsmMacVerifyAlgorithmSecondaryFamilyCustom	ECUC_Csm_00141
CsmMacVerifyCompareLength	ECUC_Csm_00142
CsmMacVerifyDataMaxLength	ECUC_Csm_00056
CsmMacVerifyProcessing	ECUC_Csm_00054

Included containers:

No Included Containers

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 perfom."
[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]: 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 #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

Problem description:

The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
There is an "i" before the "y" in "Family".

RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

Agreed solution:

Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
ECUC_Csm_00038
ECUC_Csm_00188
ECUC_Csm_00051
ECUC_Csm_00182
ECUC_Csm_00066
ECUC_Csm_00074
ECUC_Csm_00082
ECUC_Csm_00089
ECUC_Csm_00096
ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.6 Specification Item ECUC_Csm_00051

Trace References:

none

Content:

Name	CsmMacVerifyAlgorithmFamiliyFamilyCsmMacVerifyConfig.CsmMacVerifyAlgorithmFamiliyFamily
Parent Container	CsmMacVerifyConfig
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.

Multiplicity	1
Type	EcucEnumerationParamDef

Range	CRYPTO_ALGOFAM_AESCsm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_AES	0x14
	CRYPTO_ALGOFAM_BLAKE_1_256Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_1_256	0x0F
	CRYPTO_ALGOFAM_BLAKE_1_512Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_1_512	0x10
	CRYPTO_ALGOFAM_BLAKE_2s_256Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_2s_256	0x11
	CRYPTO_ALGOFAM_BLAKE_2s_512Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_2s_512	0x12
	CRYPTO_ALGOFAM_CUSTOMCsm MacVerifyConfig.CsmMac VerifyAlgorithm Familiy.CRYPTO_ALGOFAM_CUSTOM	0xFF
	CRYPTO_ALGOFAM_RIPEMD160Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_RIPEMD160	0x0E
	CRYPTO_ALGOFAM_SHA1Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA1	0x01
	CRYPTO_ALGOFAM_SHA2_224Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_224	0x02
	CRYPTO_ALGOFAM_SHA2_256Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_256	0x03
	CRYPTO_ALGOFAM_SHA2_384Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_384	0x04
	CRYPTO_ALGOFAM_SHA2_512Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_512	0x05
	CRYPTO_ALGOFAM_SHA2_512_224Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_512_224	0x06
	CRYPTO_ALGOFAM_SHA2_512_256Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_512_256	0x07
	CRYPTO_ALGOFAM_SHA3_224Csm MacVerifyConfig.CsmMac VerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA3_224	0x08

CRYPTO_ALGOMODE_CUSTOM Csm MacVerifyConfig.CsmMacVerifyAlgorithmFamily.CRYPTO_ALGOMODE_CUSTOM	0xFF		
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035

ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.7 Specification Item ECUC_Csm_00057

Trace References:

none

Content:

Container Name	CsmEncryptConfigCsmEncryptConfig
Description	Container for configuration of a CSM encryption interface. The container name serves as a symbolic name for the identifier of an encryption interface.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmEncryptAlgorithmFamiliy Family	ECUC_Csm_00182
CsmEncryptAlgorithmFamilyCustom	ECUC_Csm_00143
CsmEncryptAlgorithmKeyLength	ECUC_Csm_00191
CsmEncryptAlgorithmMode	ECUC_Csm_00060
CsmEncryptAlgorithmModeCustom	ECUC_Csm_00153
CsmEncryptAlgorithmSecondaryFamily	ECUC_Csm_00144
CsmEncryptAlgorithmSecondaryFamilyCustom	ECUC_Csm_00190
CsmEncryptDataMaxLength	ECUC_Csm_00146
CsmEncryptProcessing	ECUC_Csm_00061
CsmEncryptResultMaxLength	ECUC_Csm_00147

Included containers:

No Included Containers

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 perfom."
[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]: 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 #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035

ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.8 Specification Item ECUC_Csm_00064

Trace References:

none

Content:

Container Name	CsmDecryptConfigCsmDecryptConfig
Description	Container for configuration of a CSM decryption interface. The container name serves as a symbolic name for the identifier of an decryption interface.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmDecryptAlgorithmFamiliy Family	ECUC_Csm_00066
CsmDecryptAlgorithmFamilyCustom	ECUC_Csm_00148
CsmDecryptAlgorithmKeyLength	ECUC_Csm_00067
CsmDecryptAlgorithmMode	ECUC_Csm_00068
CsmDecryptAlgorithmModeCustom	ECUC_Csm_00152
CsmDecryptAlgorithmSecondaryFamily	ECUC_Csm_00149
CsmDecryptAlgorithmSecondaryFamilyCustom	ECUC_Csm_00150
CsmDecryptDataMaxLength	ECUC_Csm_00154
CsmDecryptProcessing	ECUC_Csm_00069
CsmDecryptResultMaxLength	ECUC_Csm_00155

Included containers:

No Included Containers

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

Problem description:

The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
There is an "i" before the "y" in "Family".

RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

Agreed solution:

Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
ECUC_Csm_00038
ECUC_Csm_00188
ECUC_Csm_00051
ECUC_Csm_00182
ECUC_Csm_00066
ECUC_Csm_00074
ECUC_Csm_00082
ECUC_Csm_00089
ECUC_Csm_00096
ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.9 Specification Item ECUC_Csm_00066

Trace References:

none

Content:

Name	CsmDecryptAlgorithmFamiliyFamilyCsmDecryptConfig.CsmDecryptAlgorithmFamiliy Family
Parent Container	CsmDecryptConfig

Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	CRYPTO_ALGOFAM_3DESCsmDecryptConfig.CsmDecryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_3DES	0x13	
	CRYPTO_ALGOFAM_AESCsmDecryptConfig.CsmDecryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_AES	0x14	
	CRYPTO_ALGOFAM_CHACHACsmDecryptConfig.CsmDecryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_CHACHA	0x15	
	CRYPTO_ALGOFAM_CUSTOMCsmDecryptConfig.CsmDecryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF	
	CRYPTO_ALGOFAM_ECIESCsmDecryptConfig.CsmDecryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_ECIES	0x1D	
	CRYPTO_ALGOFAM_RSACsmDecryptConfig.CsmDecryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_RSA	0x16	
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

Agreed solution:

Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
ECUC_Csm_00038
ECUC_Csm_00188
ECUC_Csm_00051
ECUC_Csm_00182
ECUC_Csm_00066
ECUC_Csm_00074
ECUC_Csm_00082
ECUC_Csm_00089
ECUC_Csm_00096
ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.10 Specification Item ECUC_Csm_00072

Trace References:

none

Content:

Container Name	CsmAEADEncryptConfigCsmAEADEncryptConfig
Description	Container for configuration of a CSM encryption interface. The container name serves as a symbolic name for the identifier of an encryption interface.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmAEADEncryptAlgorithmFamiliy Family	ECUC_Csm_00074

Included Parameters	
Parameter Name	SWS Item ID
CsmAEADEncryptAlgorithmFamilyCustom	ECUC_Csm_00184
CsmAEADEncryptAlgorithmKeyLength	ECUC_Csm_00075
CsmAEADEncryptAlgorithmMode	ECUC_Csm_00076
CsmAEADEncryptAlgorithmModeCustom	ECUC_Csm_00187
CsmAEADEncryptAssociatedDataMaxLength	ECUC_Csm_00159
CsmAEADEncryptCiphertextMaxLength	ECUC_Csm_00160
CsmAEADEncryptPlaintextMaxLength	ECUC_Csm_00158
CsmAEADEncryptProcessing	ECUC_Csm_00077
CsmAEADEncryptTagLength	ECUC_Csm_00161
CsmAEADEncryptKeyRef	ECUC_Csm_00157
CsmAEADEncryptQueueRef	ECUC_Csm_00156

Included containers:

No Included Containers

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.11 Specification Item ECUC_Csm_00074

Trace References:

none

Content:

Name	CsmAEADEncryptAlgorithmFamiliyFamilyCsmAEADEncryptConfig.CsmAEADEncryptAlgorithm Familiy Family		
Parent Container	CsmAEADEncryptConfig		
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	CRYPTO_ALGOFAM_3DESCsmAEADEncryptConfig.CsmAEADEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_3DES	0x13	
	CRYPTO_ALGOFAM_AESCsmAEADEncryptConfig.CsmAEADEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_AES	0x14	
	CRYPTO_ALGOFAM_CUSTOMCsmAEADEncryptConfig.CsmAEADEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF	
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035
  ECUC_Crypto_00037
  –Last change on issue 77711 comment 8–

  BW-C-Level:

Application	Specification	Bus
1	3	1

1.12 Specification Item ECUC_Csm_00076

Trace References:

none

Content:

Name	CsmAEADEncryptAlgorithmModeCsmAEADEncryptConfig.CsmAEADEncryptAlgorithmMode		
Parent Container	CsmAEADEncryptConfig		
Description	Determines the algorithm mode used for the crypto service		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	CRYPTO_ALGOFAMALGOMODE_CUSTOMCsm AEADEncryptConfig.Csm AEADEncryptAlgorithm Mode.CRYPTO_ALGOFAMALGOMODE_CUSTOM	0xFF	
	CRYPTO_ALGOMODE_GCMCsm AEADEncryptConfig.Csm AEADEncryptAlgorithm Mode.CRYPTO_ALGOMODE_GCM	0x07	
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77712: [CRYPTO] CsmAEADDecryptAlgorithmMode vs CRYPTO_ALGOFAM_CUSTOM

  Problem description:

  ECUC_Csm_00084 specifies the range of CsmAEADDecryptAlgorithmMode to [CRYPTO_ALGO*FAM*_CUSTOM, CRYPTO_ALGOMODE_GCM].
  But this should be [CRYPTO_ALGO*MODE*_CUSTOM, CRYPTO_ALGOMODE_GCM].

  Agreed solution:

  Change Range in ECUC_Csm_00084 and ECUC_Csm_00076

  Range CRYPTO_ALGOFAM_CUSTOM 0xFF
  CRYPTO_ALGOMODE_GCM 0x07

  to

  Range CRYPTO_ALGOMODE_CUSTOM 0xFF

CRYPTO_ALGOMODE_GCM 0x07
–Last change on issue 77712 comment 4–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.13 Specification Item ECUC_Csm_00080

Trace References:

none

Content:

Container Name	CsmAEADDecryptConfigCsmAEADDecryptConfig
Description	Container for configuration of a CSM decryption interface. The container name serves as a symbolic name for the identifier of an decryption interface.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmAEADDecryptAlgorithm~~Familiy~~ Family	ECUC_Csm_00082
CsmAEADDecryptAlgorithmFamilyCustom	ECUC_Csm_00185
CsmAEADDecryptAlgorithmKeyLength	ECUC_Csm_00083
CsmAEADDecryptAlgorithmMode	ECUC_Csm_00084
CsmAEADDecryptAlgorithmModeCustom	ECUC_Csm_00186
CsmAEADDecryptAssociatedDataMaxLength	ECUC_Csm_00163
CsmAEADDecryptCiphertextMaxLength	ECUC_Csm_00162
CsmAEADDecryptPlaintextMaxLength	ECUC_Csm_00165
CsmAEADDecryptProcessing	ECUC_Csm_00085
CsmAEADDecryptTagLength	ECUC_Csm_00164
CsmAEADDecryptKeyRef	ECUC_Csm_00086
CsmAEADDecryptQueueRef	ECUC_Csm_00081

Included containers:

No Included Containers

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035
  ECUC_Crypto_00037
  –Last change on issue 77711 comment 8–

  BW-C-Level:

Application	Specification	Bus
1	3	1

1.14 Specification Item ECUC_Csm_00082

Trace References:

none

Content:

Name	CsmAEADDecryptAlgorithmFamiliyFamilyCsmAEADDecryptConfig.CsmAEADDecryptAlgorithm Familiy Family

Parent Container	CsmAEADDecryptConfig		
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	CRYPTO_ALGOFAM_3DESCsm AEADDecryptConfig.Csm AEADDecryptAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_3DES	0x13	
	CRYPTO_ALGOFAM_AESCsm AEADDecryptConfig.Csm AEADDecryptAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_AES	0x14	
	CRYPTO_ALGOFAM_CUSTOMCsm AEADDecryptConfig.Csm AEADDecryptAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF	
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066

ECUC_Csm_00074
ECUC_Csm_00082
ECUC_Csm_00089
ECUC_Csm_00096
ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.15 Specification Item ECUC_Csm_00084

Trace References:

none

Content:

Name	CsmAEADDecryptAlgorithmModeCsmAEADDecryptConfig.CsmAEADDecryptAlgorithmMode		
Parent Container	CsmAEADDecryptConfig		
Description	Determines the algorithm mode used for the crypto service		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	CRYPTO_ALGOFAMALGOMODE_CUSTOMCsm AEADDecryptConfig.Csm AEADDecryptAlgorithm Mode.CRYPTO_ALGOFAMALGOMODE_CUSTOM	0xFF	
	CRYPTO_ALGOMODE_GCMCsm AEADDecryptConfig.Csm AEADDecryptAlgorithm Mode.CRYPTO_ALGOMODE_GCM	0x07	
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77712: [CRYPTO] CsmAEADDecryptAlgorithmMode vs CRYPTO_ALGOFAM_CUSTOM

  Problem description:

  ECUC_Csm_00084 specifies the range of CsmAEADDecryptAlgorithmMode to [CRYPTO_ALGO*FAM*_CUSTOM, CRYPTO_ALGOMODE_GCM].
  But this should be [CRYPTO_ALGO*MODE*_CUSTOM, CRYPTO_ALGOMODE_GCM].

  Agreed solution:

  Change Range in ECUC_Csm_00084 and ECUC_Csm_00076

  Range CRYPTO_ALGOFAM_CUSTOM 0xFF
  CRYPTO_ALGOMODE_GCM 0x07

  to

  Range CRYPTO_ALGOMODE_CUSTOM 0xFF
  CRYPTO_ALGOMODE_GCM 0x07
  –Last change on issue 77712 comment 4–

  BW-C-Level:

Application	Specification	Bus
1	3	1

1.16 Specification Item ECUC_Csm_00087

Trace References:

none

Content:

Container Name	CsmSignatureGenerateConfigCsmSignatureGenerateConfig
Description	Container for configuration of a CSM signature generation interface. The container name serves as a symbolic name for the identifier of signature generation interface.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmSignatureGenerateAlgorithmFamiliy Family	ECUC_Csm_00089
CsmSignatureGenerateAlgorithmFamilyCustom	ECUC_Csm_00166
CsmSignatureGenerateAlgorithmMode	ECUC_Csm_00091
CsmSignatureGenerateAlgorithmModeCustom	ECUC_Csm_00168
CsmSignatureGenerateAlgorithmSecondaryFamily	ECUC_Csm_00183
CsmSignatureGenerateAlgorithmSecondaryFamilyCustom	ECUC_Csm_00167
CsmSignatureGenerateDataMaxLength	ECUC_Csm_00169
CsmSignatureGenerateKeyLength	ECUC_Csm_00090
CsmSignatureGenerateProcessing	ECUC_Csm_00092
CsmSignatureGenerateResultLength	ECUC_Csm_00170

Included containers:

No Included Containers

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.17 Specification Item ECUC_Csm_00089

Trace References:

none

Content:

Name	CsmSignatureGenerateAlgorithmFamiliyFamilyCsmSignatureGenerateConfig.CsmSignatureGenerateAlgorithmFamiliy Family	
Parent Container	CsmSignatureGenerateConfig	
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.	
Multiplicity	1	
Type	EcucEnumerationParamDef	
Range	CRYPTO_ALGOFAM_BRAINPOOLCsmSignatureGenerateConfig.CsmSignatureGenerateAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_BRAINPOOL	0x15
	CRYPTO_ALGOFAM_CUSTOMCsmSignatureGenerateConfig.CsmSignatureGenerateAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF
	CRYPTO_ALGOFAM_ECCNISTCsmSignatureGenerateConfig.CsmSignatureGenerateAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_ECCNIST	0x16
	CRYPTO_ALGOFAM_ED25519CsmSignatureGenerateConfig.CsmSignatureGenerateAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_ED25519	0x14
	CRYPTO_ALGOFAM_RSACsmSignatureGenerateConfig.CsmSignatureGenerateAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_RSA	0x13

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

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035
  ECUC_Crypto_00037
  –Last change on issue 77711 comment 8–

  BW-C-Level:

Application	Specification	Bus
1	3	1

1.18 Specification Item ECUC_Csm_00094

Trace References:

none

Content:

Container Name	CsmSignatureVerifyConfigCsmSignatureVerifyConfig
Description	Container for configuration of a CSM signature verification interface. The container name serves as a symbolic name for the identifier of signature verification interface.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmSignatureVerifyAlgorithmFamiliy Family	ECUC_Csm_00096
CsmSignatureVerifyAlgorithmFamilyCustom	ECUC_Csm_00171
CsmSignatureVerifyAlgorithmMode	ECUC_Csm_00098
CsmSignatureVerifyAlgorithmModeCustom	ECUC_Csm_00174
CsmSignatureVerifyAlgorithmSecondaryFamily	ECUC_Csm_00172
CsmSignatureVerifyAlgorithmSecondaryFamilyCustom	ECUC_Csm_00173
CsmSignatureVerifyCompareLength	ECUC_Csm_00176
CsmSignatureVerifyDataMaxLength	ECUC_Csm_00175
CsmSignatureVerifyKeyLength	ECUC_Csm_00192
CsmSignatureVerifyProcessing	ECUC_Csm_00099

Included containers:

No Included Containers

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 perfom."
[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]: 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 #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

Problem description:

The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
There is an "i" before the "y" in "Family".

RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

Agreed solution:

Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
ECUC_Csm_00038
ECUC_Csm_00188
ECUC_Csm_00051
ECUC_Csm_00182
ECUC_Csm_00066
ECUC_Csm_00074
ECUC_Csm_00082
ECUC_Csm_00089
ECUC_Csm_00096
ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.19 Specification Item ECUC_Csm_00096

Trace References:

none

Content:

Name	CsmSignatureVerifyAlgorithmFamiliyFamilyCsmSignatureVerifyConfig.CsmSignatureVerifyAlgorithmFamiliy Family		
Parent Container	CsmSignatureVerifyConfig		
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	CRYPTO_ALGOFAM_BRAINPOOLCsm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BRAINPOOL	0x15	
	CRYPTO_ALGOFAM_CUSTOMCsm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF	
	CRYPTO_ALGOFAM_ECCNISTCsm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_ECCNIST	0x16	
	CRYPTO_ALGOFAM_ED25519Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_ED25519	0x14	
	CRYPTO_ALGOFAM_RSACsm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_RSA	0x13	
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035
  ECUC_Crypto_00037
  –Last change on issue 77711 comment 8–

  BW-C-Level:

Application	Specification	Bus
1	3	1

1.20 Specification Item ECUC_Csm_00103

Trace References:

none

Content:

Container Name	CsmRandomGenerateConfigCsmRandomGenerateConfig

Description	Container for configuration of a CSM random generator. The container name serves as a symbolic name for the identifier of a random generator configuration.
Configuration Parameters	

Included parameters:

Included Parameters	
Parameter Name	SWS Item ID
CsmRandomGenerateAlgorithmFamiliy Family	ECUC_Csm_00105
CsmRandomGenerateAlgorithmFamilyCustom	ECUC_Csm_00177
CsmRandomGenerateAlgorithmMode	ECUC_Csm_00107
CsmRandomGenerateAlgorithmModeCustom	ECUC_Csm_00180
CsmRandomGenerateAlgorithmSecondaryFamily	ECUC_Csm_00178
CsmRandomGenerateAlgorithmSecondaryFamilyCustom	ECUC_Csm_00179
CsmRandomGenerateProcessing	ECUC_Csm_00108
CsmRandomGenerateResultLength	ECUC_Csm_00106

Included containers:

No Included Containers

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074

ECUC_Csm_00082
ECUC_Csm_00089
ECUC_Csm_00096
ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.21 Specification Item ECUC_Csm_00105

Trace References:

none

Content:

Name	CsmRandomGenerateAlgorithmFamiliyFamilyCsmRandomGenerateConfig.CsmRandomGenerateAlgorithmFamiliy Family
Parent Container	CsmRandomGenerateConfig
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.
Multiplicity	1
Type	EcucEnumerationParamDef

Range	CRYPTO_ALGOFAM_3DESCsm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_3DES	0x13
	CRYPTO_ALGOFAM_AESCsm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_AES	0x14
	CRYPTO_ALGOFAM_BLAKE_1_256Csm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_1_256	0x0F
	CRYPTO_ALGOFAM_BLAKE_1_512Csm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_1_512	0x10
	CRYPTO_ALGOFAM_BLAKE_2s_256Csm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_2s_256	0x11
	CRYPTO_ALGOFAM_BLAKE_2s_512Csm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_2s_512	0x12
	CRYPTO_ALGOFAM_CHACHACsm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_CHACHA	0x15
	CRYPTO_ALGOFAM_CUSTOMCsm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF
	CRYPTO_ALGOFAM_RIPEMD160Csm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_RIPEMD160	0x0E
	CRYPTO_ALGOFAM_RNGCsm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_RNG	0x16
	CRYPTO_ALGOFAM_SHA1Csm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA1	0x01
	CRYPTO_ALGOFAM_SHA2_224Csm RandomGenerate Config.CsmRandom GenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_224	0x02
	CRYPTO_ALGOFAM_SHA2_256Csm RandomGenerate Config.CsmRandom	0x03

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

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035
  ECUC_Crypto_00037
  –Last change on issue 77711 comment 8–

  BW-C-Level:

Application	**Specification**	**Bus**
1	3	1

1.22 Specification Item ECUC_Csm_00111

Trace References:

none

Content:

Name	CsmCallbackIdCsmCallback.CsmCallbackId		
Parent Container	CsmCallback		
Description	Identifier of the callback function. The set of actually configured identifiers shall be consecutive and gapless.		
Multiplicity	0..1		
Type	EcucIntegerParamDef		
Range	1 0 .. 4294967295		
Default value	–		
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77049: [CRYPTO] CsmJob|Key|CallbackId configuration parameters

  Problem description:

  There are configuration parameters "CsmJob|Key|CallbackId".
  Why are these parameters specified or why are they configurable by the user?
  I think it would be more reasonable if these, only internal relevant 'values' will be auto-created by the AUTOSAR stack configuration and code generation tools, including symbolic names for this 'values' for the user.

  Especially because in my opinion it is only meaningful to number these Ids consecutively, starting from zero, incremented by one.
  Only in this way the Job, Key or Callback configurations are arrangeable in C arrays whose elements can be directly accessed (via the Id). This is the most memory and

run-time optimal solution.

(=> cmp. "Specification of Crypto Service Manager", 4.0.3, section "11.4 Configuration of the Configuration IDs")

Agreed solution:

remove note in "10.2 Containers and Configuration Parameters"
"Note: The Ids in the configuration containers shall be consecutive, gapless and shall start from zero"

[ECUC_Csm_00119] CsmJobId,
- append to description: ". The set of actually configured identifiers shall be consecutive and gapless."

[ECUC_Csm_00015] CsmKeyId,
- append to description: ". The set of actually configured identifiers shall be consecutive and gapless."
- change Range to: 0 .. 4294967295

[ECUC_Csm_00111] CsmCallbackId,
- append to description: ". The set of actually configured identifiers shall be consecutive and gapless."
- change Range to: 0 .. 4294967295
–Last change on issue 77049 comment 7–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.23 Specification Item ECUC_Csm_00113

Trace References:

none

Content:

Name	CsmMainFunctionPeriodCsmGeneral.CsmMainFunctionPeriod	
Description	Specifies the period of main function Csm_MainFunction in seconds.	
Multiplicity	0..1	
Type	EcucFloatParamDef	
Range	]0 .. INF[	

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

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy'n'paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

  SWS_Csm_00969 ... the enumeration of the return value is disarranged
  SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"
  SWS_Csm_00970 ... even if return value is VOID, the 'return value' entry is NOT 'None' as it is for all other functions returning 'void'

  SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
  SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
  SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
  SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
  SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.24 Specification Item ECUC_Csm_00119

Trace References:

none

Content:

Name	CsmJobIdCsmJob.CsmJobId
Parent Container	CsmJob
Description	Identifier of the CSM job. The set of actually configured identifiers shall be consecutive and gapless.
Multiplicity	1

Type	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
Range	0 .. 4294967295		
Default value	–		
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77049: [CRYPTO] CsmJob|Key|CallbackId configuration parameters

  Problem description:

  There are configuration parameters "CsmJob|Key|CallbackId".
  Why are these parameters specified or why are they configurable by the user?
  I think it would be more reasonable if these, only internal relevant 'values' will be auto-created by the AUTOSAR stack configuration and code generation tools, including symbolic names for this 'values' for the user.

  Especially because in my opinion it is only meaningful to number these Ids consecutively, starting from zero, incremented by one.
  Only in this way the Job, Key or Callback configurations are arrangeable in C arrays whose elements can be directly accessed (via the Id). This is the most memory and run-time optimal solution.

  (=> cmp. "Specification of Crypto Service Manager", 4.0.3, section "11.4 Configuration of the Configuration IDs")

  Agreed solution:

  remove note in "10.2 Containers and Configuration Parameters"
  "Note: The Ids in the configuration containers shall be consecutive, gapless and shall start from zero"

  [ECUC_Csm_00119] CsmJobId,
  - append to description: ". The set of actually configured identifiers shall be consecutive and gapless."

[ECUC_Csm_00015] CsmKeyId,
- append to description: ". The set of actually configured identifiers shall be consecutive and gapless."
- change Range to: 0 .. 4294967295

[ECUC_Csm_00111] CsmCallbackId,
- append to description: ". The set of actually configured identifiers shall be consecutive and gapless."
- change Range to: 0 .. 4294967295
–Last change on issue 77049 comment 7–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.25 Specification Item ECUC_Csm_00131

Trace References:

none

Content:

Name	CsmHashAlgorithmMode		
Description	Determines the algorithm mode used for the crypto service		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	CRYPTO_ALGOMODE_CUSTOM	0xFF	
	CRYPTO_ALGOMODE_NOT_SET	0x00	
Default value	CRYPTO_ALGOMODE_NOT_SET		
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76337: Wrong defaultValue for CsmHashAlgorithmMode

Problem description:

Name: Robert Sakretz
Phone:
Role: WP-M

Description/Motivation:

The default value for "CsmHashAlgorithmMode" does not match any of the available options:

current default value: CRYPTO_ALGOFAM_NOT_SET

available options: CRYPTO_ALGOMODE_NOT_SET, CRYPTO_ALGOMODE_CUSTOM

Agreed solution:

change default value of CsmHashAlgorithmMode to CRYPTO_ALGOMODE_NOT_SET.

BW-C-Level:

Application	Specification	Bus
1	1	1

1.26 Specification Item ECUC_Csm_00172

Trace References:

none

Content:

Name	CsmSignatureVerifyAlgorithmSecondaryFamilyCsmSignatureVerifyConfig.CsmSignatureVerifyAlgorithmSecondaryFamily
Parent Container	CsmSignatureVerifyConfig
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.
Multiplicity	1
Type	EcucEnumerationParamDef

Range	CRYPTO_ALGOFAM_BLAKE_1_256 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_BLAKE_1_256	0x0F
	CRYPTO_ALGOFAM_BLAKE_1_512 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_BLAKE_1_512	0x10
	CRYPTO_ALGOFAM_BLAKE_2s_256 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_BLAKE_2s_256	0x11
	CRYPTO_ALGOFAM_BLAKE_2s_512 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_BLAKE_2s_512	0x12
	CRYPTO_ALGOFAM_CUSTOM Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF
	CRYPTO_ALGOFAM_NOT_SET Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_NOT_SET	0x00
	CRYPTO_ALGOFAM_RIPEMD160 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_RIPEMD160	0x0E
	CRYPTO_ALGOFAM_SHA1 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_SHA1	0x01
	CRYPTO_ALGOFAM_SHA2_224 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_SHA2_224	0x02
	CRYPTO_ALGOFAM_SHA2_256 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_SHA2_256	0x03
	CRYPTO_ALGOFAM_SHA2_384 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_SHA2_384	0x04
	CRYPTO_ALGOFAM_SHA2_512 Csm SignatureVerifyConfig.Csm SignatureVerifyAlgorithm SecondaryFam-	0x05

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

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77723: [CRYPTO] CRYPTO_ALGOFAM_BLAKE

  Problem description:

  Value CRYPTO_ALGOFAM_BLAKE (0x0F) is listed in enums ECUC_Csm_00172/CsmSignatureVerifyAlgorithmSecondaryFamily and ECUC_Csm_00183/CsmSignatureGenerateAlgorithmSecondaryFamily. But this specific value is not included in SWS_Csm_01047/Crypto_AlgorithmFamilyType. Instead there are multiple BLAKE variants.

  Agreed solution:

  for ECUC_Csm_00172 and ECUC_Csm_00183:

  rename CRYPTO_ALGOFAM_BLAKE into CRYPTO_ALGOFAM_BLAKE_1_256

  add to the other algofam:
  CRYPTO_ALGOFAM_BLAKE_1_512 0x10
  CRYPTO_ALGOFAM_BLAKE_2s_256 0x11
  CRYPTO_ALGOFAM_BLAKE_2s_512 0x12
  –Last change on issue 77723 comment 10–

  BW-C-Level:

Application	Specification	Bus
1	4	1

1.27 Specification Item ECUC_Csm_00182

Trace References:

none

Content:

Name	CsmEncryptAlgorithmFamiliyFamilyCsmEncryptConfig.CsmEncryptAlgorithmFamiliy Family		
Parent Container	CsmEncryptConfig		
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.		
Multiplicity	1		
Type	EcucEnumerationParamDef		
Range	CRYPTO_ALGOFAM_3DESCsmEncryptConfig.CsmEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_3DES	0x13	
	CRYPTO_ALGOFAM_AESCsmEncryptConfig.CsmEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_AES	0x14	
	CRYPTO_ALGOFAM_CHACHACsmEncryptConfig.CsmEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_CHACHA	0x15	
	CRYPTO_ALGOFAM_CUSTOMCsmEncryptConfig.CsmEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF	
	CRYPTO_ALGOFAM_ECIESCsmEncryptConfig.CsmEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_ECIES	0x1D	
	CRYPTO_ALGOFAM_RSACsmEncryptConfig.CsmEncryptAlgorithmFamiliyFamily.CRYPTO_ALGOFAM_RSA	0x16	
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

Agreed solution:

Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
ECUC_Csm_00038
ECUC_Csm_00188
ECUC_Csm_00051
ECUC_Csm_00182
ECUC_Csm_00066
ECUC_Csm_00074
ECUC_Csm_00082
ECUC_Csm_00089
ECUC_Csm_00096
ECUC_Csm_00105

SWS_CryptoDriver:
Change Familiy to Family:
ECUC_Crypto_00035
ECUC_Crypto_00037
–Last change on issue 77711 comment 8–

BW-C-Level:

Application	Specification	Bus
1	3	1

1.28 Specification Item ECUC_Csm_00183

Trace References:

none

Content:

Name	CsmSignatureGenerateAlgorithmSecondaryFamilyCsmSignatureGenerateConfig.CsmSignatureGenerateAlgorithmSecondaryFamily
Parent Container	CsmSignatureGenerateConfig
Description	Determines the algorithm mode used for the crypto service
Multiplicity	1
Type	EcucEnumerationParamDef

Range	CRYPTO_ALGOFAM_~~BLAKE~~BLAKE_1_256Csm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_BLAKE_1_256	0x0F
	CRYPTO_ALGOFAM_BLAKE_1_512Csm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_BLAKE_1_512	0x10
	CRYPTO_ALGOFAM_BLAKE_2s_256Csm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_BLAKE_2s_256	0x11
	CRYPTO_ALGOFAM_BLAKE_2s_512Csm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_BLAKE_2s_512	0x12
	CRYPTO_ALGOFAM_CUSTOMCsm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF
	CRYPTO_ALGOFAM_NOT_SETCsm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_NOT_SET	0x00
	CRYPTO_ALGOFAM_RIPEMD160Csm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_RIPEMD160	0x0E
	CRYPTO_ALGOFAM_SHA1Csm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_SHA1	0x01
	CRYPTO_ALGOFAM_SHA2_224Csm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_SHA2_224	0x02
	CRYPTO_ALGOFAM_SHA2_256Csm SignatureGenerate Config.CsmSignature GenerateAlgorithm SecondaryFamily.CRYPTO_ALGOFAM_SHA2_256	0x03

Default value	CsmSignatureGenerateConfig.CsmSignatureGenerateAlgorithmSecondaryFamily.CRYPTO_ALGOFAM_NOT_SET		
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77723: [CRYPTO] CRYPTO_ALGOFAM_BLAKE

  Problem description:

  Value CRYPTO_ALGOFAM_BLAKE (0x0F) is listed in enums ECUC_Csm_00172/CsmSignatureVerifyAlgorithmSecondaryFamily and ECUC_Csm_00183/CsmSignatureGenerateAlgorithmSecondaryFamily. But this specific value is not included in SWS_Csm_01047/Crypto_AlgorithmFamilyType. Instead there are multiple BLAKE variants.

  Agreed solution:

  for ECUC_Csm_00172 and ECUC_Csm_00183:

  rename CRYPTO_ALGOFAM_BLAKE into CRYPTO_ALGOFAM_BLAKE_1_256

  add to the other algofam:
  CRYPTO_ALGOFAM_BLAKE_1_512 0x10
  CRYPTO_ALGOFAM_BLAKE_2s_256 0x11
  CRYPTO_ALGOFAM_BLAKE_2s_512 0x12
  –Last change on issue 77723 comment 10–

  BW-C-Level:

Application	Specification	Bus
1	4	1

1.29 Specification Item ECUC_Csm_00188

Trace References:

none

Content:

Name	CsmMacGenerateAlgorithmFamiliyFamilyCsmMacGenerateConfig.CsmMacGenerateAlgorithm Familiy Family
Parent Container	CsmMacGenerateConfig
Description	Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.
Multiplicity	1
Type	EcucEnumerationParamDef

Range	CRYPTO_ALGOFAM_3DESCsm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_3DES	0x13
	CRYPTO_ALGOFAM_AESCsm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_AES	0x14
	CRYPTO_ALGOFAM_BLAKE_1_256Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_1_256	0x0F
	CRYPTO_ALGOFAM_BLAKE_1_512Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_1_512	0x10
	CRYPTO_ALGOFAM_BLAKE_2s_256Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_2s_256	0x11
	CRYPTO_ALGOFAM_BLAKE_2s_512Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_BLAKE_2s_512	0x12
	CRYPTO_ALGOFAM_CHACHACsm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_CHACHA	0x15
	CRYPTO_ALGOFAM_CUSTOMCsm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_CUSTOM	0xFF
	CRYPTO_ALGOFAM_RIPEMD160Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_RIPEMD160	0x0E
	CRYPTO_ALGOFAM_RNGCsm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_RNG	0x16
	CRYPTO_ALGOFAM_SHA1Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA1	0x01
	CRYPTO_ALGOFAM_SHA2_224Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_224	0x02
	CRYPTO_ALGOFAM_SHA2_256Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_256	0x03
	CRYPTO_ALGOFAM_SHA2_384Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_384	0x04
	CRYPTO_ALGOFAM_SHA2_512Csm MacGenerateConfig.Csm MacGenerateAlgorithm FamiliyFamily.CRYPTO_ALGOFAM_SHA2_512	0x05
	CRYPTO_ALGOFAM_SHA2_512_224Csm	0x06

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

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77711: [CRYPTO] Csm<Service>AlgorithmFamiliy

  Problem description:

  The name of all configuration parameters CsmHash|MacGenerate|MacVerify|...AlgorithmFamiliy is not correctly written.
  There is an "i" before the "y" in "Family".

  RfC 76783 mentioned this for CsmMacGenerateAlgorithmFamiliy only.

  Agreed solution:

  Change Csm<Service>AlgorithmFamiliy to Csm<Service>AlgorithmFamily in the following ECUCs:
  ECUC_Csm_00038
  ECUC_Csm_00188
  ECUC_Csm_00051
  ECUC_Csm_00182
  ECUC_Csm_00066
  ECUC_Csm_00074
  ECUC_Csm_00082
  ECUC_Csm_00089
  ECUC_Csm_00096
  ECUC_Csm_00105

  SWS_CryptoDriver:
  Change Familiy to Family:
  ECUC_Crypto_00035
  ECUC_Crypto_00037
  –Last change on issue 77711 comment 8–

  BW-C-Level:

Application	Specification	Bus
1	3	1

1.30 Specification Item ECUC_Csm_00191

Trace References:

none

Content:

Name	CsmEncryptAlgorithmKeyLengthCsmEncryptConfig.CsmEncryptAlgorithmKeyLength		
Parent Container	CsmEncryptConfig		
Description	Size of the encryption key in bytes		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	1 .. 4294967295		
Default value	–		
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

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 perfom."
[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]: 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 #78327: [CRYPTO] CsmSignatureVerifyConfig incomplete

  Problem description:

  The ECUC_Csm_00087/CsmSignatureGenerateConfig container contains following parameter:
  - ECUC_Csm_00090/CsmSignatureGenerateKeyLength

  In ECUC_Csm_00094/CsmSignatureVerifyConfig container an corresponding parameter is missing.

  Agreed solution:

  In CsmSignatureVerifyConfig chapter add new SWS Item after ECUC_Csm_00173:

  SWS Item ECUC_Csm_XXXXX :
  Name CsmSignatureVerifyKeyLength
  Description Size of the signature verify key in bytes
  Multiplicity 1
  Type EcucIntegerParamDef
  Range 1 .. 4294967295
  Default value –
  Post-Build Variant Value false
  Multiplicity Configuration Class
  Pre-compile time X All Variants
  Link time –
  Post-build time –
  Value Configuration Class
  Pre-compile time X All Variants
  Link time –
  Post-build time –
  Scope / Dependency scope: local

  *ECUC_Csm_xxxxx: choose not already taken one (at writing this 00192 is

free)
–Last change on issue 78327 comment 4–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.31 Specification Item ECUC_Csm_00192

Trace References:

none

Content:

Name	CsmSignatureVerifyKeyLengthCsmSignatureVerifyConfig.CsmSignatureVerifyKeyLength		
Parent Container	CsmSignatureVerifyConfig		
Description	Size of the signature verify key in bytes		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	1 .. 4294967295		
Default value	–		
Post-Build Variant Value	false		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

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 perfom."
[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]: 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 #78276: [CRYPTO] CsmEncryptConfig incomplete

Problem description:

The ECUC_Csm_00064/CsmDecryptConfig container contains following parameter:
- CsmDecryptAlgorithmKeyLength

In ECUC_Csm_00057/CsmEncryptConfig container an corresponding parameter is missing.

Agreed solution:

In CsmEncryptConfig chapter add new SWS Item after ECUC_Csm_00143:

SWS Item ECUC_Csm_xxxxx :
Name CsmEncryptAlgorithmKeyLength
Description Size of the encryption key in bytes
Multiplicity 1
Type EcucIntegerParamDef
Range 1 .. 4294967295
Default value –
Post-Build Variant Value false
Multiplicity Configuration Class Pre-compile time X All Variants
Link time –
Post-build time –
Value Configuration Class Pre-compile time X All Variants
Link time –
Post-build time –
Scope / Dependency scope: local

*ECUC_Csm_xxxxx: choose not already taken one (at writing this 00191 is

free)
–Last change on issue 78276 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.32 Specification Item ECUC_Csm_00193

Trace References:

none

Content:

Name	CsmMacVerifyAlgorithmKeyLengthCsmMacVerifyConfig.CsmMacVerifyAlgorithmKeyLength		
Parent Container	CsmMacVerifyConfig		
Description	Size of the MAC key in bytes		
Multiplicity	1		
Type	EcucIntegerParamDef		
Range	1 .. 4294967295		
Default value	–		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

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 "associatedDataL-

ength"
[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 perfom."
[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]: 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

1.33 Specification Item ECUC_Csm_00194

Trace References:

none

Content:

Name	CsmMacVerifyAlgorithmModeCustomCsmMacVerifyConfig.CsmMacVerifyAlgorithmModeCustom		
Parent Container	CsmMacVerifyConfig		
Description	Name of the custom algorithm mode used for the crypto service		
Multiplicity	0..1		
Type	EcucStringParamDef		
Default value	–		
maxLength	–		
minLength	–		
regularExpression	–		
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

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 perfom."
[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]: 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 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

1.34 Specification Item ECUC_Csm_00195

Trace References:

none

Content:

Name	CsmMacVerifyAlgorithmModeCsmMacVerifyConfig.CsmMacVerifyAlgorithmMode
Parent Container	CsmMacVerifyConfig
Description	Determines the algorithm mode used for the crypto service
Multiplicity	1
Type	EcucEnumerationParamDef

Range	CRYPTO_ALGOMODE_CMAC	0x10	CsmMacVerifyConfig.CsmMacVerifyAlgorithmMode.CRYPTO_ALGOMODE_CMAC
	CRYPTO_ALGOMODE_CTRDRBG	0x12	CsmMacVerifyConfig.CsmMacVerifyAlgorithmMode.CRYPTO_ALGOMODE_CTRDRBG
	CRYPTO_ALGOMODE_CUSTOM	0xff	CsmMacVerifyConfig.CsmMacVerifyAlgorithmMode.CRYPTO_ALGOMODE_CUSTOM
	CRYPTO_ALGOMODE_GMAC	0x11	CsmMacVerifyConfig.CsmMacVerifyAlgorithmMode.CRYPTO_ALGOMODE_GMAC
	CRYPTO_ALGOMODE_HMAC	0x0f	CsmMacVerifyConfig.CsmMacVerifyAlgorithmMode.CRYPTO_ALGOMODE_HMAC
	CRYPTO_ALGOMODE_NOT_SET	0x00	CsmMacVerifyConfig.CsmMacVerifyAlgorithmMode.CRYPTO_ALGOMODE_NOT_SET
	CRYPTO_ALGOMODE_SIPHASH_2_4	0x17	CsmMacVerifyConfig.CsmMacVerifyAlgorithmMode.CRYPTO_ALGOMODE_SIPHASH_2_4
	CRYPTO_ALGOMODE_SIPHASH_4_8	0x18	CsmMacVerifyConfig.CsmMacVerifyAlgorithmMode.CRYPTO_ALGOMODE_SIPHASH_4_8
Multiplicity Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Value Configuration Class	Pre-compile time	X	All Variants
	Link time	–	
	Post-build time	–	
Scope / Dependency	scope: local		

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 perfom."
[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]: 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 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

1.35 Specification Item SWS_Csm_00037

Trace References:

none

Content:

If a synchronous job is issued and the priority is less greater than the highest priority available in the queue, the CSM shall return E_BUSYdisable processing new jobs from the queue until the next call of the main function.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements

[SWS_Csm_00932]: assigned to two different requirements
[SWS_Csm_00934]: assigned to two different requirements
–Last change on issue 76440 comment 19–

Agreed solution:

SWS_Csm_00037 -> new ID for second
SWS_Csm_00828 -> new ID for first
SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_00930 -> new ID for first
SWS_Csm_00932 -> new ID for first
SWS_Csm_00934 -> new ID for first
–Last change on issue 76440 comment 15–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.36 Specification Item SWS_Csm_00168

Trace References:

none

Content:

Service name:	Csm_SymBlockEncryptStart (obsolete)Csm_SymBlockEncryptStart	
Syntax:	Std_ReturnType Csm_SymBlockEncryptStart(Csm_ConfigIdType cfgId, const Csm_SymKeyType* keyPtr)	
Service ID[hex]:	0x10	
Sync/Async:	Sync or Async, dependent on configuration (CSM0557_Conf)	
Reentrancy:	Non Reentrant	
Parameters (in):	cfgIdCsm_SymBlockEncryptStart.cfgId	holds the identifier of the CSM module configuration which has to be used during the symmetrical block encryption computation.
	keyPtrCsm_SymBlockEncryptStart.keyPtr	holds a pointer to the key which has to be used during the symmetrical block encryption computation.

Parameters (inout):	None	
Parameters (out):	None	
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CSM_E_BUSY: request failed, service is still busy
Description:	This function is deprecated. Sets the key and initialization vector for symmetrical encryption. Tags: atp.Status=obsolete	

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 perfom."
[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]: 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

1.37 Specification Item SWS_Csm_00173

Trace References:

none

Content:

Service name:	Csm_SymBlockEncryptUpdate (obsolete)Csm_SymBlockEncryptUpdate

Syntax:	Std_ReturnType Csm_SymBlockEncryptUpdate(Csm_ConfigIdType cfgId, const uint8* plainTextPtr, uint32 plainTextLength, uint8* cipherTextPtr, uint32* cipherTextLengthPtr)	
Service ID[hex]:	0x11	
Sync/Async:	Sync or Async, dependent on configuration (CSM0557_Conf)	
Reentrancy:	Non Reentrant	
Parameters (in):	cfgIdCsm_SymBlockEncryptUpdate.cfgId	Holds the identifier of the CSM module configuration that has to be used during the operation.
	plainTextPtrCsm_SymBlockEncryptUpdate.plainTextPtr	holds a pointer to the plain text that shall be encrypted.
	plainTextLengthCsm_SymBlockEncryptUpdate.plainTextLength	contains the length of the plain text in bytes
Parameters (inout):	cipherTextLengthPtrCsm_SymBlockEncryptUpdate.cipherTextLengthPtr	holds a pointer to a memory location in which the length information is stored. On calling this function this parameter shall contain the size of the buffer provided by cipherTextPtr. When the request has finished, the amount of data that has been encrypted shall be stored.
Parameters (out):	cipherTextPtrCsm_SymBlockEncryptUpdate.cipherTextPtr	holds a pointer to the memory location which will hold the encrypted text.
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CSM_E_BUSY: request failed, service is still busy CSM_E_SMALL_BUFFER: the provided buffer is too small to store the result
Description:	This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer. Tags: atp.Status=obsolete	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy’n’paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

SWS_Csm_00969 ... the enumeration of the return value is disarranged
SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"
SWS_Csm_00970 ... even if return value is VOID, the 'return value' entry is NOT 'None' as it is for all other functions returning 'void'

SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.38 Specification Item SWS_Csm_00180

Trace References:

none

Content:

Service name:	Csm_SymBlockEncryptFinish (obsolete)Csm_SymBlockEncryptFinish	
Syntax:	Std_ReturnType Csm_SymBlockEncryptFinish(Csm_ConfigIdType cfgId)	
Service ID[hex]:	0x12	
Sync/Async:	Sync or Async, dependent on configuration (CSM0557_Conf)	
Reentrancy:	Non Reentrant	
Parameters (in):	cfgIdCsm_SymBlockEncryptFinish.cfgId	Holds the identifier of the CSM module configuration that has to be used during the operation.
Parameters (inout):	None	
Parameters (out):	None	
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CSM_E_BUSY: request failed, service is still busy
Description:	This function is deprecated. Finishes the symmetrical encrypt service. Tags: atp.Status=obsolete	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy'n'paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

SWS_Csm_00969 ... the enumeration of the return value is disarranged
SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"
SWS_Csm_00970 ... even if return value is VOID, the ’return value’ entry is NOT ’None’ as it is for all other functions returning ’void’

SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.39 Specification Item SWS_Csm_00206

Trace References:

none

Content:

Service name:	Csm_SymEncryptStart (obsolete)Csm_SymEncryptStart	
Syntax:	Std_ReturnType Csm_SymEncryptStart(Csm_ConfigIdType cfgId, const Csm_SymKeyType* keyPtr, const uint8* InitVectorPtr, uint32 InitVectorLength)	
Service ID[hex]:	0x16	
Sync/Async:	Sync or Async, dependent on configuration (CSM0557_Conf)	
Reentrancy:	Non Reentrant	
Parameters (in):	cfgIdCsm_SymEncryptStart.cfgId	holds the identifier of the CSM module configuration which has to be used during the symmetrical encryption computation.
	keyPtrCsm_SymEncryptStart.keyPtr	holds a pointer to the key which has to be used during the symmetrical encryption computation
	InitVectorPtrCsm_SymEncryptStart.InitVectorPtr	holds a pointer to the initialisation vector which has to be used during the symmetrical encryption computation
	InitVectorLengthCsm_SymEncryptStart.InitVectorLength	holds the length of the initialisation vector which has to be used during the symmetrical encryption computation
Parameters (inout):	None	
Parameters (out):	None	
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CSM_E_BUSY: request failed, service is still busy
Description:	This interface shall be used to initialize the symmetrical encrypt service of the CSM module. If the service state is "active", the function shall return with "CSM_E_BUSY". Otherwise, this function shall store the given configuration information which is identified by "cfgId", call the function Cry_<Primitive>Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cry_<Primitive>Start returned successfully, the service state has to be set to "active"function is deprecated. Sets the key and initialization vector for symmetrical encryption. Tags: atp.Status=obsolete	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy'n'paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

  SWS_Csm_00969 ... the enumeration of the return value is disarranged
  SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"
  SWS_Csm_00970 ... even if return value is VOID, the 'return value' entry is NOT 'None' as it is for all other functions returning 'void'

  SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
  SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
  SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
  SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
  SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

  ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

  Agreed solution:

  SWS_Csm_00206: replace description with:
  This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
  Tags: atp.Status=obsolete

  SWS_Csm_00212: replace description with:
  This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
  Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.40 Specification Item SWS_Csm_00212

Trace References:

none

Content:

Service name:	Csm_SymEncryptUpdate (obsolete)Csm_SymEncryptUpdate	
Syntax:	Std_ReturnType Csm_SymEncryptUpdate(Csm_ConfigIdType cfgId, const uint8* plainTextPtr, uint32 plainTextLength, uint8* cipherTextPtr, uint32* cipherTextLengthPtr)	
Service ID[hex]:	0x17	
Sync/Async:	Sync or Async, dependent on configuration (CSM0557_Conf)	
Reentrancy:	Non Reentrant	
Parameters (in):	cfgIdCsm_SymEncryptUpdate.cfgId	Holds the identifier of the CSM module configuration that has to be used during the operation.
	plainTextPtrCsm_SymEncrypt Update.plainTextPtr	holds a pointer to the plain text that shall be encrypted.
	plainTextLengthCsm_SymEncrypt Update.plainTextLength	contains the length of the plain text in bytes

Parameters (inout):	cipherTextLengthPtrCsm_SymEncrypt Update.cipherTextLengthPtr	holds a pointer to a memory location in which the length information is stored. On calling this function this parameter shall contain the size of the buffer provided by cipherTextPtr. When the request has finished, the amount of data that has been encrypted shall be stored.
Parameters (out):	cipherTextPtrCsm_SymEncrypt Update.cipherTextPtr	holds a pointer to the memory location which will hold the encrypted text.
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CSM_E_BUSY: request failed, service is still busy CSM_E_SMALL_BUFFER: the provided buffer is too small to store the result
Description:	This interface shall be used to feed the symmetrical encryption function is deprecated. Feeds the symmetrical encrypt service with the input data . If the service state is "idle", the function has to return with "E_NOT_OK". Otherwise, this function shall call the function Cry_<Primitive>Update of the primitive which is identified by the stored configuration information and return the value returned by that function. The encryption process is done by the underlying primitiveand store the ciphertext in the memory location pointed by the ciphertext pointer. Tags: atp.Status=obsolete	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy’n’paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

  SWS_Csm_00969 ... the enumeration of the return value is disarranged
  SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"
  SWS_Csm_00970 ... even if return value is VOID, the ’return value’ entry is NOT ’None’ as it is for all other functions returning ’void’

  SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing

SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.41 Specification Item SWS_Csm_00221

Trace References:

none

Content:

Service name:	Csm_SymEncryptFinish (obsolete)Csm_SymEncryptFinish	
Syntax:	Std_ReturnType Csm_SymEncryptFinish(Csm_ConfigIdType cfgId, uint8* cipherTextPtr, uint32* cipherTextLengthPtr)	
Service ID[hex]:	0x18	
Sync/Async:	Sync or Async, dependent on configuration (CSM0557_Conf)	
Reentrancy:	Non Reentrant	
Parameters (in):	cfgIdCsm_SymEncryptFinish.cfgId	Holds the identifier of the CSM module configuration that has to be used during the operation.
Parameters (inout):	cipherTextLengthPtrCsm_SymEncryptFinish.cipherTextLengthPtr	holds a pointer to a memory location in which the length information is stored. On calling this function this parameter shall contain the size of the buffer provided by cipherTextPtr. When the request has finished, the amount of data that has been encrypted shall be stored.
Parameters (out):	cipherTextPtrCsm_SymEncryptFinish.cipherTextPtr	holds a pointer to the memory location which will hold the encrypted text.
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CSM_E_BUSY: request failed, service is still busy CSM_E_SMALL_BUFFER: the provided buffer is too small to store the result
Description:	This interface shall be used to finish the symmetrical encryption function is deprecated. Finishes the symmetrical encrypt service. If the service state is "idle", the function has to return with "E_NOT_OK". Otherwise, this function shall call the function Cry_<Primitive>Finish of the primitive which is identified by the stored configuration information and return the value returned by that function. Tags: The encryption process is done by the underlying primitive.atp.Status=obsolete	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy’n’paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

SWS_Csm_00969 ... the enumeration of the return value is disarranged
SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"
SWS_Csm_00970 ... even if return value is VOID, the 'return value' entry is NOT 'None' as it is for all other functions returning 'void'

SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.42 Specification Item SWS_Csm_00455

Trace References:

SRS_BSW_00359, SRS_BSW_00360

Content:

Service name:	Csm_<Service>CallbackNotification (obsolete)Csm_CallbackNotificationService	
Syntax:	void Csm_<Service>CallbackNotification(Std_ReturnType Result)	
Service ID[hex]:	0x79	
Sync/Async:	Synchronous	
Reentrancy:	Non Reentrant	
Parameters (in):	ResultCsm_CallbackNotification Service.Result	Contains the result of the cryptographic operation
Parameters (inout):	None	
Parameters (out):	None	
Return value:	None	
Description:	This function is deprecated. This function shall call the callback function as given in the configuration of the service <Service> with the argument given by "Result". Tags: atp.Status=obsolete	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy'n'paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

  SWS_Csm_00969 ... the enumeration of the return value is disarranged
  SWS_Csm_00455 ... contains introducing sentence "This function is deprecated."

without "Tags: atp.Status=obsolete"
SWS_Csm_00970 ... even if return value is VOID, the 'return value' entry is NOT 'None' as it is for all other functions returning 'void'

SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):

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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.43 Specification Item SWS_Csm_00489

Trace References:

SRS_BSW_00406, SRS_BSW_00337, SRS_CryptoStack_00087, SRS_CryptoStack_00088

Content:

The following table specifies which DET error values shall be reported for each API call:

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

1.44 Specification Item SWS_Csm_00539

Trace References:

SRS_BSW_00406, SRS_BSW_00337, SRS_BSW_00385, SRS_CryptoStack_00087, SRS_CryptoStack_00088

Content:

API call	Error condition	DET related error value
All APIs except Csm_Init()	CSM is not initialized	CSM_E_UNINIT
Csm_Init	Initialization of CSM failed	CSM_E_INIT_FAILED
All APIs that have a pointer as parameter	Pointer is Nullpointer	CSM_E_PARAM_POINTER In case a NULL pointer has been passed, the API service shall report development error to DET if enabled and return immediately without any further action.
All APIs that have a keyId as parameter	keyId is out of range	CSM_E_PARAM_HANDLE

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

1.45 Specification Item SWS_Csm_00659

Trace References:

none

Content:

If the initialization of the CSM module fails, the CSM shall report CSM_E_INIT_FAILED to the DET when CsmDevErrorDetect is true.

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

1.46 Specification Item SWS_Csm_00775

Trace References:

SRS_Csm_00066

Content:

Name	CsmHash_{Primitive}CsmHash	
Comment	Interface to execute the hash calculation.	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmHash/CsmHashConfig.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmHash.CancelJob	
Comments	Cancels the job.

CancelJobCsmHash.CancelJob		
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	

HashCsmHash.Hash			
Comments	Streaming approach of the hash calculation.		
Variation	–		
Parameters	dataBufferCsmHash.Hash.dataBuffer	Comment	Contains the data to be hashed.
		Type	Csm_HashDataType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmHash/CsmHashConfig.SHORT-NAME)}
		Direction	IN
	dataLengthCsmHash.Hash.dataLength	Comment	Contains the length in bytes of the data to be hashed.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmHash.Hash.resultBuffer	Comment	Contains the data of the hash.
		Type	Csm_HashResultType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmHash/CsmHashConfig.SHORT-NAME)}
		Direction	INOUT OUT
	resultLengthCsmHash.Hash.resultLength	Comment	Contains the length in bytes of the hash.
		Type	uint32
		Variation	–
		Direction	IN INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77779: Incorrect Direction sementics for CSM_Hash

  Problem description:

Contradicting direction for RTE and C interfaces of Csm_Hash functionality.
C Interface with semantic correct paramters: resultPtr (out), resultLengthPtr (inout)
RTE Interface with incorreect paramters: resultBuffer (INOUT) (OUT is correct), resultLength (IN) (INOUT is correct)

Agreed solution:

SWS_Csm_00946:

RTE interface Parameters needs an update in direction: resultBuffer (OUT), resultLength(INOUT)
–Last change on issue 77779 comment 3–

BW-C-Level:

Application	**Specification**	**Bus**
4	4	1

1.47 Specification Item SWS_Csm_00776

Trace References:

SRS_Csm_00066

Content:

Name	CsmMacGenerate_{Primitive}CsmMacGenerate	
Comment	Interface to execute the MAC generation.	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerate Config.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmMacGenerate.CancelJob		
Comments	Cancels the job.	
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	
	CSM_E_BUSY	failed, service is still busy

MacGenerateCsmMacGenerate.MacGenerate			
Comments	Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer.		
Variation	–		
Parameters	dataBufferCsmMacGenerate.MacGenerate.dataBuffer	Comment	Contains the length in bytes of the data from which a MAC shall be generated of.
		Type	Csm_MacGenerateDataType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig.SHORT-NAME)}
		Direction	IN
	dataLengthCsmMacGenerate.MacGenerate.dataLength	Comment	Contains the length in bytes of the data from which a MAC shall be generated of.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmMacGenerate.MacGenerate.resultBuffer	Comment	Contains the data of the MAC.
		Type	Csm_MacGenerateResultType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig.SHORT-NAME)}
		Direction	OUT
	resultLengthCsmMacGenerate.MacGenerate.resultLength	Comment	Contains the length in bytes of the MAC.
		Type	uint32
		Variation	–
		Direction	INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77264: [CRYPTO] possible errors of "CancelJob" operation of Client-Server-Interfaces

  Problem description:

  The specifications of the possible errors of the "CancelJob" operation of the Client-Server-Interfaces are varying.

Sometimes there is CSM_E_BUSY defined, sometimes not. Sometimes there are actually no possible errors specified.

Agreed solution:

——————————-
For 4.3.1
- Remove in every CancelJob Operation the Possible Error: "CSM_E_BUSY failed, service is still busy"
in the following Items:
[SWS_Csm_009000]
[SWS_Csm_00936]
[SWS_Csm_00947]
[SWS_Csm_00903]

- [SWS_Csm_00943]
Add Possible Errors to Operation CancelJob
Possible Errors
0 E_OK Operation successful
1 E_NOT_OK –
–Last change on issue 77264 comment 21–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.48 Specification Item SWS_Csm_00777

Trace References:

SRS_Csm_00066

Content:

Name	CsmMacVerify_{Primitive}CsmMacVerify	
Comment	Interface to execute the MAC verification.	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerify Config.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmMacVerify.CancelJob		
Comments	Cancels the job.	
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	
	CSM_E_BUSY	failed, service is still busy

MacVerifyCsmMacVerify.MacVerify			
Comments	Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer.		
Variation	–		
Parameters	dataBufferCsmMac Verify.MacVerify.dataBuffer	Comment	Contains the length in bytes of the data from which a MAC shall be generated of.
		Type	Csm_MacVerifyData Type_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/CsmMac Verify/CsmMacVerify Config.SHORT-NAME)}
		Direction	IN
	dataLengthCsmMac Verify.MacVerify.dataLength	Comment	Contains the length in bytes of the data for whichs MAC shall be verified.
		Type	uint32
		Variation	–
		Direction	IN
	compareBufferCsmMac Verify.MacVerify.compare Buffer	Comment	Contains the MAC to be verified.
		Type	Csm_MacVerifyCompare Type_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/CsmMac Verify/CsmMacVerify Config.SHORT-NAME)}
		Direction	IN
	compareLengthCsmMac Verify.MacVerify.compare Length	Comment	Contains the length in BITS of the MAC to be verified.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmMac Verify.MacVerify.resultBuffer	Comment	Contains the data of the MAC.
		Type	Crypto_VerifyResultType
		Variation	–
		Direction	OUT

MacVerifyCsmMacVerify.MacVerify		
Possible Errors	E_OK	Operation successful
	E_NOT_OK	
	CSM_E_BUSY	failed, service is still busy
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77264: [CRYPTO] possible errors of "CancelJob" operation of Client-Server-Interfaces

  Problem description:

  The specifications of the possible errors of the "CancelJob" operation of the Client-Server-Interfaces are varying.
  Sometimes there is CSM_E_BUSY defined, sometimes not. Sometimes there are actually no possible errors specified.

  Agreed solution:

  —————————————-
  For 4.3.1
  - Remove in every CancelJob Operation the Possible Error: "CSM_E_BUSY failed, service is still busy"
  in the following Items:
  [SWS_Csm_009000]
  [SWS_Csm_00936]
  [SWS_Csm_00947]
  [SWS_Csm_00903]

  - [SWS_Csm_00943]
  Add Possible Errors to Operation CancelJob
  Possible Errors
  0 E_OK Operation successful
  1 E_NOT_OK –
  –Last change on issue 77264 comment 21–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.49 Specification Item SWS_Csm_00783

Trace References:

SRS_Csm_00066

Content:

Name	CsmSymDecrypt (obsolete)CsmSymDecrypt	
Comment	Interface to execute the symmetric decryption. Tags: atp.Status=obsolete	
IsService	true	
Variation	–	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

SymDecryptFinish (obsolete)CsmSymDecrypt.SymDecryptFinish			
Comments	This operation is deprecated. Finishes the symmetrical decrypt service. Tags: atp.Status=obsolete		
Variation	–		
Parameters	plainTextBufferCsmSymDecrypt.SymDecryptFinish.plainTextBuffer	Comment	Contains the data of the encrypted plaintext.
		Type	SymDecryptResultBuffer
		Variation	–
		Direction	OUT
	plainTextLengthCsmSymDecrypt.SymDecryptFinish.plainTextLength	Comment	Contains the length in bytes of the data of the encrypted plaintext.
		Type	uint32
		Variation	–
		Direction	INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

SymDecryptStart (obsolete)CsmSymDecrypt.SymDecryptStart

SymDecryptStart (obsolete)CsmSymDecrypt.SymDecryptStart			
Comments	This operation is deprecated. Sets the key for symmetrical decryption. Tags: atp.Status=obsolete		
Variation	–		
Parameters	keyCsmSymDecrypt.SymDecryptStart.key	Comment	Identifier of the key.
		Type	Csm_SymKeyType
		Variation	–
		Direction	IN
	InitVectorBufferCsmSymDecrypt.SymDecryptStart.InitVectorBuffer	Comment	Contains the data of the initiation vector.
		Type	SymDecryptInitVectorBuffer
		Variation	–
		Direction	IN
	InitVectorLengthCsmSymDecrypt.SymDecryptStart.InitVectorLength	Comment	Contains the length in bytes of the data of the initiation vector.
		Type	uint32
		Variation	–
		Direction	IN
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	

SymDecryptUpdate (obsolete)CsmSymDecrypt.SymDecryptUpdate	
Comments	This operation is deprecated. Feeds the symmetrical decrypt service with the input data and store the decrypted plaintext. Tags: atp.Status=obsolete
Variation	–

SymDecryptUpdate (obsolete)CsmSymDecrypt.SymDecryptUpdate			
Parameters	cipherTextBufferCsmSymDecrypt.SymDecryptUpdate.cipherTextBuffer	Comment	Contains the data to be decrypted
		Type	SymDecryptDataBuffer
		Variation	–
		Direction	IN
	cipherTextLengthCsmSymDecrypt.SymDecryptUpdate.cipherTextLength	Comment	Contains the length in bytes of the data to be encrypted.
		Type	uint32
		Variation	–
		Direction	IN
	plainTextBufferCsmSymDecrypt.SymDecryptUpdate.plainTextBuffer	Comment	Contains the data of the encrypted plaintext.
		Type	SymDecryptResultBuffer
		Variation	–
		Direction	OUT
	plainTextLengthCsmSymDecrypt.SymDecryptUpdate.plainTextLength	Comment	Contains the length in bytes of the data of the encrypted plaintext.
		Type	uint32
		Variation	–
		Direction	INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy'n'paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

  SWS_Csm_00969 ... the enumeration of the return value is disarranged
  SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"

SWS_Csm_00970 ... even if return value is VOID, the 'return value' entry is NOT 'None' as it is for all other functions returning 'void'

SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.50 Specification Item SWS_Csm_00786

Trace References:

SRS_Csm_00066

Content:

Name	CsmSignatureGenerate_{Primitive}CsmSignatureGenerate	
Comment	–	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmSignatureGenerate/CsmSignature GenerateConfig.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmSignatureGenerate.CancelJob		
Comments	Cancels the job.	
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	
	CSM_E_BUSY	failed, service is still busy

SignatureGenerateCsmSignatureGenerate.SignatureGenerate	
Comments	Streaming approach of the signature generation.
Variation	–

SignatureGenerateCsmSignatureGenerate.SignatureGenerate			
Parameters	dataBufferCsmSignatureGenerate.SignatureGenerate.dataBuffer	Comment	Contains the length in bytes of the data from which the signature shall be generated.
		Type	Csm_SignatureGenerateDataType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmSignatureGenerate/CsmSignatureGenerateConfig.SHORT-NAME)}
		Direction	IN
	dataLengthCsmSignatureGenerate.SignatureGenerate.dataLength	Comment	Contains the length in bytes of the data from which the signature shall be generated.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmSignatureGenerate.SignatureGenerate.resultBuffer	Comment	Contains the signature.
		Type	Csm_SignatureGenerateResultType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmSignatureGenerate/CsmSignatureGenerateConfig.SHORT-NAME)}
		Direction	OUT
	resultLengthCsmSignatureGenerate.SignatureGenerate.resultLength	Comment	Contains the length in bytes of the signature.
		Type	uint32
		Variation	–
		Direction	INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77264: [CRYPTO] possible errors of "CancelJob" operation of Client-Server-Interfaces

  Problem description:

  The specifications of the possible errors of the "CancelJob" operation of the Client-Server-Interfaces are varying.
  Sometimes there is CSM_E_BUSY defined, sometimes not. Sometimes there are actually no possible errors specified.

Agreed solution:

——————————–

For 4.3.1
- Remove in every CancelJob Operation the Possible Error: "CSM_E_BUSY failed, service is still busy"
in the following Items:
[SWS_Csm_009000]
[SWS_Csm_00936]
[SWS_Csm_00947]
[SWS_Csm_00903]

- [SWS_Csm_00943]
Add Possible Errors to Operation CancelJob
Possible Errors
0 E_OK Operation successful
1 E_NOT_OK –
–Last change on issue 77264 comment 21–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.51 Specification Item SWS_Csm_00787

Trace References:

SRS_Csm_00066

Content:

Name	CsmSignatureVerify (obsolete)CsmSignatureVerify_Obsolete	
Comment	Interface to execute the signature verification. Tags: atp.Status=obsolete	
IsService	true	
Variation	–	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY

Operations:

SignatureVerifyFinish (obsolete)CsmSignatureVerify_Obsolete.SignatureVerifyFinish

SignatureVerifyFinish (obsolete)CsmSignatureVerify_Obsolete.SignatureVerifyFinish			
Comments	This function operation is deprecated. Finishes the signature verification and stores the verification result. Tags: atp.Status=obsolete		
Variation	–		
Parameters	signatureBufferCsmSignatureVerify_Obsolete.SignatureVerifyFinish.signatureBuffer	Comment	Contains the signature to be verified.
		Type	SignatureVerifyCompareSignatureBuffer
		Variation	–
		Direction	IN
	signatureLengthCsmSignatureVerify_Obsolete.SignatureVerifyFinish.signatureLength	Comment	Contains the length in bytes of the signature to be verified.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmSignatureVerify_Obsolete.SignatureVerifyFinish.resultBuffer	Comment	Contains the result of the signature verification.
		Type	Csm_VerifyResultType
		Variation	–
		Direction	OUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	

SignatureVerifyStart (obsolete)CsmSignatureVerify_Obsolete.SignatureVerifyStart			
Comments	This operation is deprecated. Sets the key for signature verification. Tags: atp.Status=obsolete		
Variation	–		
Parameters	keyCsmSignatureVerify_Obsolete.SignatureVerifyStart.key	Comment	This operation is deprecated. Sets the key for signature verification.
		Type	Csm_AsymPublicKeyType
		Variation	–
		Direction	IN
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	

SignatureVerifyUpdate (obsolete)CsmSignatureVerify_Obsolete.SignatureVerifyUpdate	
Comments	This operation is deprecated. Feeds the signature verification service with the input data. Tags: atp.Status=obsolete

SignatureVerifyUpdate (obsolete)CsmSignatureVerify_Obsolete.SignatureVerifyUpdate			
Variation	–		
Parameters	dataBufferCsmSignatureVerify_Obsolete.SignatureVerifyUpdate.dataBuffer	Comment	Contains the data for whichs signature shall be verified.
		Type	SignatureVerifyDataBuffer
		Variation	–
		Direction	IN
	dataLengthCsmSignatureVerify_Obsolete.SignatureVerifyUpdate.dataLength	Comment	Contains the length in bytes of the data for whichs signature shall be verified.
		Type	uint32
		Variation	–
		Direction	IN
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy'n'paste errors

  Problem description:

  SWS_Csm_00206 ... description does not match other deprecated start APIs
  SWS_Csm_00212 ... description does not match other deprecated update APIs
  SWS_Csm_00221 ... description does not match other deprecated finish APIs

  SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
  SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

  SWS_Csm_00969 ... the enumeration of the return value is disarranged
  SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"
  SWS_Csm_00970 ... even if return value is VOID, the 'return value' entry is NOT 'None' as it is for all other functions returning 'void'

  SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
  SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
  SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
  SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in

"operationis"
SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	**Specification**	**Bus**
1	1	1

1.52 Specification Item SWS_Csm_00828

Trace References:

SRS_CryptoStack_00086

Content:

Development Error Types

Type of error	Related error code	Value [hex]
API request called with invalid parameter (Nullpointer)	CSM_E_PARAM_POINTER	0x01
API request called before initialization of CSM module	CSM_E_UNINIT	0x05
Initialization of CSM module failed	CSM_E_INIT_FAILED	0x07
Requested service is not initialized	CSM_E_SERVICE_NOT_STARTED	0x09

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_00930 -> new ID for first
  SWS_Csm_00932 -> new ID for first
  SWS_Csm_00934 -> new ID for first
  –Last change on issue 76440 comment 15–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.53 Specification Item SWS_Csm_00830

Trace References:

SRS_CryptoStack_00087

Content:

If the API returns CRYPTO_E_SMALL_BUFFER, additonally CSM_E_SMALL_BUFFER shall be reported to the Det when CsmDevErrorDetect is true.

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

1.54 Specification Item SWS_Csm_009000

Trace References:

SRS_CryptoStack_00090

Content:

Name	CsmMacGenerate_{Primitive}CsmMacGenerate	
Comment	Interface to execute the MAC generation.	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmMacGenerate.CancelJob		
Comments	Cancels the job.	
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	
	CSM_E_BUSY	failed, service is still busy

MacGenerateCsmMacGenerate.MacGenerate	
Comments	Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer.
Variation	–

MacGenerateCsmMacGenerate.MacGenerate			
Parameters	dataBufferCsmMacGenerate.MacGenerate.dataBuffer	Comment	Contains the length in bytes of the data from which a MAC shall be generated of.
		Type	Csm_MacGenerateDataType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig.SHORT-NAME)}
		Direction	IN
	dataLengthCsmMacGenerate.MacGenerate.dataLength	Comment	Contains the length in bytes of the data from which a MAC shall be generated of.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmMacGenerate.MacGenerate.resultBuffer	Comment	Contains the data of the MAC.
		Type	Csm_MacGenerateResultType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig.SHORT-NAME)}
		Direction	OUT
	resultLengthCsmMacGenerate.MacGenerate.resultLength	Comment	Contains the length in bytes of the MAC.
		Type	uint32
		Variation	–
		Direction	INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77264: [CRYPTO] possible errors of "CancelJob" operation of Client-Server-Interfaces

Problem description:

The specifications of the possible errors of the "CancelJob" operation of the Client-Server-Interfaces are varying.
Sometimes there is CSM_E_BUSY defined, sometimes not. Sometimes there are actually no possible errors specified.

Agreed solution:

——————————-
For 4.3.1
- Remove in every CancelJob Operation the Possible Error: "CSM_E_BUSY failed, service is still busy"
in the following Items:
[SWS_Csm_009000]
[SWS_Csm_00936]
[SWS_Csm_00947]
[SWS_Csm_00903]

- [SWS_Csm_00943]
Add Possible Errors to Operation CancelJob
Possible Errors
0 E_OK Operation successful
1 E_NOT_OK –
–Last change on issue 77264 comment 21–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.55 Specification Item SWS_Csm_00925

Trace References:

none

Content:

The application shall be able to call arbitrary often Csm_<Service>() with the operation mode CRYPTO_OPERATIONMODE_UPDATE arbitrary often, but at least one time, to feed the job's crypto primitive with input data.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77371: [CRYPTO] discrepance in number of calls for Csm_<Service>() functions with CRYPTO_OPERATIONMODE_UPDATE

  Problem description:

  [SWS_Csm_00925] specifies that the application shall be able to call arbitrary often Csm_<Service>() with the operation mode CRYPTO_OPERATIONMODE_UPDATE to feed the jobs crypto primitive with input data.

  "Arbitrary often" means 0 to infinite times, so it would be possible to call Csm_<Service>() with
  CRYPTO_OPERATIONMODE_START directly followed by CRYPTO_OPERATIONMODE_FINISH ... maybe to calculate a MAC for no data.

  [SWS_Csm_00024] and others specify that CRYPTO_OPERATIONMODE_FINISH is only a valid argument from within the update state which means that at least ONE call with CRYPTO_OPERATIONMODE_UPDATE is necessary before CRYPTO_OPERATIONMODE_FINISH is permitted.

  Please clarify!

  Agreed solution:

  [SWS_Csm_00925]
  The application shall be able to call Csm_<Service>() with the operation mode CRYPTO_OPERATIONMODE_UPDATE arbitrary often, but at least one time, to feed the job's crypto primitive with input data.
  ()
  –Last change on issue 77371 comment 8–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.56 Specification Item SWS_Csm_00930

Trace References:

none

Content:

Each crypto primitive configuration shall be realized as a constant structure of type Crypto_PrimitiveInfoType.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_00930 -> new ID for first
  SWS_Csm_00932 -> new ID for first
  SWS_Csm_00934 -> new ID for first
  –Last change on issue 76440 comment 15–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.57 Specification Item SWS_Csm_00932

Trace References:

none

Content:

Each job primitive configuration shall be realized as a constant structure of type Crypto_JobPrimitiveInfoType.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_00930 -> new ID for first
  SWS_Csm_00932 -> new ID for first
  SWS_Csm_00934 -> new ID for first
  –Last change on issue 76440 comment 15–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.58 Specification Item SWS_Csm_00934

Trace References:

SRS_CryptoStack_00090, SRS_CryptoStack_00091

Content:

Name	{Job}_MacVerifyCallback}_CallbackNotificationCsm.MacVerify CallbackNotification		
Kind	ProvidedRequiredPort	Interface	CsmMacVerify_{Primitive} CallbackNotification
Description	Port for a job to verify a MAC the callback notification.		

Port Defined Argument Value(s)

Type	uint32	
Value	({ecuc(Csm/CsmJobs/CsmJob. CsmJobId)}	
Type	Crypto_OperationModeType	
Value	CRYPTO_OPERATIONMODE_SINGLECALL	
Variation	({ecuc(Csm/CsmJobsCallbacks/CsmJob.CsmJobUsePort)} == TRUE) && ({ecuc(CsmCallback/CsmJobs/CsmJob.CsmJobPrimitiveRef -> CsmPrimitives/CsmMacVerifyCallbackFunc)} != NULL) Job Callback = {ecuc(Csm/CsmPrimitivesCallbacks/CsmMacVerifyCallback/CsmMacVerifyConfig.SHORT-NAME)} Primitive = {ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerifyConfigCallbackFunc.SHORT-NAME)}	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_01083 -> correction already available (refer to .../Z-

GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_00930 -> new ID for first
SWS_Csm_00932 -> new ID for first
SWS_Csm_00934 -> new ID for first
–Last change on issue 76440 comment 15–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.59 Specification Item SWS_Csm_00936

Trace References:

SRS_CryptoStack_00090

Content:

Name	CsmMacVerify_{Primitive}CsmMacVerify	
Comment	Interface to execute the MAC verification.	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerify Config.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmMacVerify.CancelJob		
Comments	Cancels the job.	
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	
	CSM_E_BUSY	failed, service is still busy

MacVerifyCsmMacVerify.MacVerify	
Comments	Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer.
Variation	–

MacVerifyCsmMacVerify.MacVerify			
Parameters	dataBufferCsmMac Verify.MacVerify.dataBuffer	Comment	Contains the length in bytes of the data from which a MAC shall be generated of.
		Type	Csm_MacVerifyData Type_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/CsmMac Verify/CsmMacVerify Config.SHORT-NAME)}
		Direction	IN
	dataLengthCsmMac Verify.MacVerify.dataLength	Comment	Contains the length in bytes of the data for whichs MAC shall be verified.
		Type	uint32
		Variation	–
		Direction	IN
	compareBufferCsmMac Verify.MacVerify.compare Buffer	Comment	Contains the MAC to be verified.
		Type	Csm_MacVerifyCompare Type_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/CsmMac Verify/CsmMacVerify Config.SHORT-NAME)}
		Direction	IN
	compareLengthCsmMac Verify.MacVerify.compare Length	Comment	Contains the length in BITS of the MAC to be verified.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmMac Verify.MacVerify.resultBuffer	Comment	Contains the data of the MAC.
		Type	Crypto_VerifyResultType
		Variation	–
		Direction	OUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77264: [CRYPTO] possible errors of "CancelJob" operation of Client-Server-Interfaces

  Problem description:

The specifications of the possible errors of the "CancelJob" operation of the Client-Server-Interfaces are varying.
Sometimes there is CSM_E_BUSY defined, sometimes not. Sometimes there are actually no possible errors specified.

Agreed solution:

——————————-
For 4.3.1
- Remove in every CancelJob Operation the Possible Error: "CSM_E_BUSY failed, service is still busy"
in the following Items:
[SWS_Csm_009000]
[SWS_Csm_00936]
[SWS_Csm_00947]
[SWS_Csm_00903]

- [SWS_Csm_00943]
Add Possible Errors to Operation CancelJob
Possible Errors
0 E_OK Operation successful
1 E_NOT_OK –
–Last change on issue 77264 comment 21–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.60 Specification Item SWS_Csm_00946

Trace References:

SRS_CryptoStack_00090

Content:

Name	CsmHash_{Primitive}CsmHash	
Comment	Interface to execute the hash calculation.	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmHash/CsmHashConfig.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmHash.CancelJob		
Comments	Cancels the job.	
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	

HashCsmHash.Hash			
Comments	Streaming approach of the hash calculation.		
Variation	–		
Parameters	dataBufferCsmHash.Hash.dataBuffer	Comment	Contains the data to be hashed.
		Type	Csm_HashDataType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmHash/CsmHashConfig.SHORT-NAME)}
		Direction	IN
	dataLengthCsmHash.Hash.dataLength	Comment	Contains the length in bytes of the data to be hashed.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmHash.Hash.resultBuffer	Comment	Contains the data of the hash.
		Type	Csm_HashResultType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmHash/CsmHashConfig.SHORT-NAME)}
		Direction	INOUT OUT
	resultLengthCsmHash.Hash.resultLength	Comment	Contains the length in bytes of the hash.
		Type	uint32
		Variation	–
		Direction	IN INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77779: Incorrect Direction sementics for CSM_Hash

Problem description:

Contradicting direction for RTE and C interfaces of Csm_Hash functionality.
C Interface with semantic correct paramters: resultPtr (out), resultLengthPtr (inout)
RTE Interface with incorreect paramters: resultBuffer (INOUT) (OUT is correct), resultLength (IN) (INOUT is correct)

Agreed solution:

SWS_Csm_00946:

RTE interface Parameters needs an update in direction: resultBuffer (OUT), resultLength(INOUT)
–Last change on issue 77779 comment 3–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.61 Specification Item SWS_Csm_00947

Trace References:

SRS_CryptoStack_00906

Content:

Name	CsmEncrypt_{Primitive}CsmEncrypt	
Comment	Interface to execute the encryption.	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmEncrypt/CsmEncrypt Config.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmEncrypt.CancelJob	
Comments	Cancels the job.
Variation	–

CancelJobCsmEncrypt.CancelJob		
Possible Errors	E_OK	Operation successful
	E_NOT_OK	
	CSM_E_BUSY	failed, service is still busy

EncryptCsmEncrypt.Encrypt			
Comments	Encrypts the given data and store the ciphertext in the memory location pointed by the result pointer.		
Variation	–		
Parameters	dataBufferCsm Encrypt.Encrypt.dataBuffer	Comment	Contains the data to be encrypted.
		Type	Csm_EncryptData Type_{Crypto}
		Variation	Crypto ={ecuc(Csm/Csm Primitives/CsmEncrypt/Csm Encrypt Config.SHORT-NAME)}
		Direction	IN
	dataLengthCsm Encrypt.Encrypt.dataLength	Comment	Contains the length in bytes of the data to be encrypted.
		Type	uint32
		Variation	–
		Direction	IN
	resultCsm Encrypt.Encrypt.result	Comment	Contains the data of the cipher.
		Type	Csm_EncryptResult Type_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/CsmEncrypt/Csm Encrypt Config.SHORT-NAME)}
		Direction	OUT
	resultLengthCsm Encrypt.Encrypt.resultLength	Comment	Contains the length in bytes of the cipher.
		Type	uint32
		Variation	–
		Direction	INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77264: [CRYPTO] possible errors of "CancelJob" operation of Client-Server-Interfaces

  Problem description:

  The specifications of the possible errors of the "CancelJob" operation of the Client-Server-Interfaces are varying.
  Sometimes there is CSM_E_BUSY defined, sometimes not. Sometimes there are actually no possible errors specified.

  Agreed solution:

  ——————————-
  For 4.3.1
  - Remove in every CancelJob Operation the Possible Error: "CSM_E_BUSY failed, service is still busy"
  in the following Items:
  [SWS_Csm_009000]
  [SWS_Csm_00936]
  [SWS_Csm_00947]
  [SWS_Csm_00903]

  - [SWS_Csm_00943]
  Add Possible Errors to Operation CancelJob
  Possible Errors
  0 E_OK Operation successful
  1 E_NOT_OK –
  –Last change on issue 77264 comment 21–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.62 Specification Item SWS_Csm_00951

Trace References:

SRS_CryptoStack_00008

Content:

If the key material itself consist of more than one element , it shall be stored as PKCS#8 in the key element.

Examples are asymmetric algorithms like in RSA where the key consists of a modulus and an exponent or and an ECC key which consists of the X and Y coordinatesFor each key element that contains cryptographic key material, the format of the provided key shall be specified in the configuration used for data exchange, e.g. for Csm_KeyElementGet() or Csm_KeyElementSet().The key formats supported by a specific crypto driver are part of the pre-configuration information that comes along with the crypto driver.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77661: Definition for asymmetric key formats

  Problem description:

  Name: Armin Happel

  Description/Motivation:
  Currently, the AUTOSAR crypto stack specifies to provide asymmetric key material in PKCS# 8 format only [see SWS_CSM_00951]. However, the standard is not precise enough and defines only the usage of private key material. Optionally, public key material can be provided in addition. This provides the lack of definition in the AUTOSAR stack, that public keys cannot be provided for certain algorithms, such as signature verification.
  This RFC extends the current definition so that also public key material can be provided to the crypto stack.

  Agreed solution:

  See attachment: https://bugzilla.autosar.org/attachment.cgi?id=4617
  –Last change on issue 77661 comment 29–

  BW-C-Level:

Application	Specification	Bus
1	4	1

1.63 Specification Item SWS_Csm_00953

Trace References:

SRS_CryptoStack_00008

Content:

The following key formats are available:

CRYPTO_KE_FORMAT_BIN_OCTET	Key provided as octet value in binary form1.
CRYPTO_KE_FORMAT_BIN_SHEKEYS	Combined input/output keys for SHE operation (M1+M2+M3) and (M4+M5).
CRYPTO_KE_FORMAT_BIN_IDENT_PRIVATEKEY_ PKCS8	Private key material in ASN.1 coded form (BER coding) with identification. The data is provided in binary form, not, e.g. as a BASE64 string.
CRYPTO_KE_FORMAT_BIN_IDENT_PUBLICKEY	Public key material in ASN.1 coded form (BER coding) with identification. The data is provided in binary form, not, e.g. as a BASE64 string.
CRYPTO_KE_FORMAT_BIN _RSA_PRIVATEKEY	Private key material in ASN.1 coded form (BER coding). The key material is provided in binary form, not, e.g. as a BASE64 string.
CRYPTO_KE_FORMAT_BIN _RSA_PUBLICKEY	Public key material in ASN.1 coded form (BER coding). The key material is provided in binary form, not, e.g. as a BASE64 string.
CRYPTO_KE_FORMAT_BIN_CERT_X509_V3	TBD
CRYPTO_KE_FORMAT_BIN_CERT_CVC	TBD

A binary Octet is the integer representation in base 256. A large value can be splitted into his factors:

x = x xLen-1 * 256xLen-1 + xxLen-2 * 256xLen-2 + ... + x1 * 256 + x0. where 0 <= xi < 256.

Let the Octet Xi have the integer value xxLen-i for 1 <= i <= xLen. The octet is then

X = X1 X2 .. XxLen

Rationale: An asymmetric key can either be provided with or without identification. The identification is used to uniquely identify the key itself that is provided, so that the key parser can check if the key material is appropriate or not. Without identification, the key material must correspond to the format that is specified for this key. Following IETF standards, the identification of a key is provided as an object identifier (OID) as part of the ASN.1 description.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77661: Definition for asymmetric key formats

  Problem description:

  Name: Armin Happel

Description/Motivation:
Currently, the AUTOSAR crypto stack specifies to provide asymmetric key material in PKCS# 8 format only [see SWS_CSM_00951]. However, the standard is not precise enough and defines only the usage of private key material. Optionally, public key material can be provided in addition. This provides the lack of definition in the AUTOSAR stack, that public keys cannot be provided for certain algorithms, such as signature verification.
This RFC extends the current definition so that also public key material can be provided to the crypto stack.

Agreed solution:

See attachment: https://bugzilla.autosar.org/attachment.cgi?id=4617
–Last change on issue 77661 comment 29–

BW-C-Level:

Application	Specification	Bus
1	4	1

1.64 Specification Item SWS_Csm_00966

Trace References:

SRS_CrytptoStack_00028

Content:

Service name:	Csm_KeyExchangeCalcPubValCsm_KeyExchangeCalcPubVal	
Syntax:	Std_ReturnType Csm_KeyExchangeCalcPubVal(uint32 keyId, uint8* publicValuePtr, uint32* publicValueLengthPtr)	
Service ID[hex]:	0x6c	
Sync/Async:	Synchronous	
Reentrancy:	Reentrant, but not for same keyId	
Parameters (in):	keyIdCsm_KeyExchangeCalcPubVal.keyId	Holds the identifier of the key which shall be used for the key exchange protocol.
Parameters (inout):	publicValueLengthPtrCsm_KeyExchangeCalcPubVal.publicValueLengthPtr	Holds a pointer to the memory location in which the public value length information is stored. On calling this function, this parameter shall contain the size of the buffer provided by publicValuePtr. When the request has finished, the actual length of the returned value shall be stored.
Parameters (out):	publicValuePtrCsm_KeyExchangeCalcPubVal.publicValuePtr	Contains the pointer to the data where the public value shall be stored.

Return value:	Std_ReturnType	Wrong return values - here are the correct ones: E_OK: request successful E_NOT_OK: request failed CRYPTO_E_KEY_NOT_VALID: request failed, the key's state is "invalid" CRYPTO_E_SMALL_BUFFER: the provided buffer is too small to store the result.
Description:	Calculates the public value of the current user for the key exchange and stores the public key in the memory location pointed by the public value 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 perfom."
[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]: 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

1.65 Specification Item SWS_Csm_00969

Trace References:

none

Content:

Service name:	Csm_KeyElementCopyCsm_KeyElementCopy

Syntax:	Std_ReturnType Csm_KeyElementCopy(const uint32 keyId, const uint32 keyElementId, const uint32 targetKeyId, const uint32 targetKeyElementId)	
Service ID[hex]:	0x71	
Sync/Async:	Synchronous	
Reentrancy:	Reentrant, but not for the same keyId	
Parameters (in):	keyIdCsm_KeyElementCopy.keyId	Holds the identifier of the key whose key element shall be the source element.
	keyElementIdCsm_KeyElementCopy.keyElementId	Holds the identifier of the key element which shall be the source for the copy operation.
	targetKeyIdCsm_KeyElementCopy.targetKeyId	Holds the identifier of the key whose key element shall be the destination element.
	targetKeyElementIdCsm_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 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_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. 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 #76936: [CRYPTO] miscellaneous typos, inconsistencies & copy'n'paste errors

  Problem description:

SWS_Csm_00206 ... description does not match other deprecated start APIs
SWS_Csm_00212 ... description does not match other deprecated update APIs
SWS_Csm_00221 ... description does not match other deprecated finish APIs

SWS_Csm_00173 ... description does not include "Tags: atp.Status=obsolete"
SWS_Csm_00180 ... description does not include "Tags: atp.Status=obsolete"
SWS_Csm_00221 ... description does not include "Tags: atp.Status=obsolete"
SWS_Csm_00455 ... description does not include "Tags: atp.Status=obsolete"

SWS_Csm_00969 ... the enumeration of the return value is disarranged
SWS_Csm_00455 ... contains introducing sentence "This function is deprecated." without "Tags: atp.Status=obsolete"
SWS_Csm_00970 ... even if return value is VOID, the 'return value' entry is NOT 'None' as it is for all other functions returning 'void'

SWS_Csm_00775 / HashStart (obsolete) ... introducing sentence "This operation is deprecated." is missing
SWS_Csm_00777 / MacVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."
SWS_Csm_00783 / SymDecryptFinish ... shall be obsolete with correct comment
SWS_Csm_00786 / SignatureGenerateStart (obsolete) ... add space in comment in "operationis"
SWS_Csm_00787 / SignatureVerifyFinish (obsolete) ... introducing sentence "This function is deprecated." shall be replaced with "This operation is deprecated."

ECUC_Csm_00113 ... "Post-Build Variant Value" element is missing

Agreed solution:

SWS_Csm_00206: replace description with:
This function is deprecated. Sets the key and initialization vector for symmetrical encryption.
Tags: atp.Status=obsolete

SWS_Csm_00212: replace description with:
This function is deprecated. Feeds the symmetrical encrypt service with the input data and store the ciphertext in the memory location pointed by the ciphertext pointer.
Tags: atp.Status=obsolete

SWS_Csm_00221: replace description with:
This function is deprecated. Finishes the symmetrical encrypt service.
Tags: atp.Status=obsolete

SWS_Csm_00173: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00180: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00221: add obsolete status after description: "Tags: atp.Status=obsolete"
SWS_Csm_00455: add obsolete status after description: "Tags: atp.Status=obsolete"

SWS_Csm_00969: re-arrange and replace return value with ("E_BUSY: Request Failed, Crypto Driver Object is Busy" is duplicated):
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_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.
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.

SWS_Csm_00970: replace "Return value: void – " with "Return value: None"

SWS_Csm_00775 / HashStart (obsolete): Add introducing sentence to the description: "This operation is deprecated."

SWS_Csm_00777 / MacVerifyFinish (obsolete): Replace Comments: "function" with "operation"

SWS_Csm_00783 / SymDecryptFinish: Add (obsolete) to operation name "SymDecryptFinish (obsolete)"
and add obsolete statur to comment:
"Tags: atp.Status=obsolete"

SWS_Csm_00786 / SignatureGenerateStart (obsolete): typo in comment: replace "operationis" with "operation is"

SWS_Csm_00787 / SignatureVerifyFinish (obsolete): Replace in Comments: "function" with "operation"

ECUC_Csm_00113: add "Post-Build Variant Value: false"

-remove all "DEPRECATED: This interface will be removed in the next major release!"
–Last change on issue 76936 comment 9–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.66 Specification Item SWS_Csm_00973

Trace References:

none

Content:

If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead

3. CryIf_RandomGenerate

Could you please check and solve it?

Agreed solution:

[SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

add note to 7.2.2.2.1 after [SWS_Csm_00939]:
Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):

step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.67 Specification Item SWS_Csm_00982

Trace References:

SRS_CryptoStack_00022

Content:

Service name:	Csm_MacGenerateCsm_MacGenerate	
Syntax:	Std_ReturnType Csm_MacGenerate(uint32 jobId, Crypto_OperationModeType mode, const uint8* dataPtr, uint32 dataLength, uint8* macPtr, uint32* macLengthPtr)	
Service ID[hex]:	0x60	
Sync/Async:	Asynchronous Sync or Async, dependend dependent on the job configuration	
Reentrancy:	Reentrant	
Parameters (in):	jobIdCsm_MacGenerate.jobId	Holds the identifier of the job using the CSM service.
	modeCsm_MacGenerate.mode	Indicates which operation mode(s) to perfom.
	dataPtrCsm_MacGenerate.dataPtr	Contains the pointer to the data for which the MAC shall be computed.
	dataLengthCsm_MacGenerate.dataLength	Contains the number of bytes to be hashed.
Parameters (inout):	macLengthPtrCsm_MacGenerate.macLengthPtr	Holds a pointer to the memory location in which the output length in bytes is stored. On calling this function, this parameter shall contain the size of the buffer provided by macPtr. When the request has finished, the actual length of the returned MAC shall be stored.
Parameters (out):	macPtrCsm_MacGenerate.macPtr	Contains the pointer to the data where the MAC shall be stored.

Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CRYPTO_E_BUSY: request failed, service is still busy CRYPTO_E_QUEUE_FULL: request failed, the queue is full CRYPTO_E_KEY_NOT_VALID: request failed, the key's state is "invalid" CRYPTO_E_SMALL_BUFFER: the provided buffer is too small to store the result.
Description:	Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer.	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77560: [CRYPTO] Typo in Csm_MacGenerate Sync/Async

  Problem description:

  In SWS_Csm_00982 the API function Csm_MacGenerate is specified to "Asynchronous or Async". This should be "Sync or Async".

  Agreed solution:

  [SWS_Csm_00982] replace value of "Sync/Async" row from "Asynchronous or Async, dependend on the job configuration" to "Sync or Async, dependend on the job configuration"
  –Last change on issue 77560 comment 2–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.68 Specification Item SWS_Csm_00986

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = dataPtr, job->jobPrimitiveInputOutput.inputLength = dataLength,

job->jobPrimitiveInputOutput.outputPtr = resultPtr,

job->jobPrimitiveInputOutput.outputLengthPtr = resultLengthPtr.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead
  3. CryIf_RandomGenerate

  Could you please check and solve it?

  Agreed solution:

  [SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

  add note to 7.2.2.2.1 after [SWS_Csm_00939]:
  Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.69 Specification Item SWS_Csm_00990

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = dataPtr,

job->jobPrimitiveInputOutput.inputLength = dataLength,

job->jobPrimitiveInputOutput.outputPtr = resultPtr,

job->jobPrimitiveInputOutput.outputLengthPtr = resultLengthPtr.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead
  3. CryIf_RandomGenerate

  Could you please check and solve it?

  Agreed solution:

  [SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

  add note to 7.2.2.2.1 after [SWS_Csm_00939]:
  Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job.

Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.70 Specification Item SWS_Csm_00992

Trace References:

SRS_CryptoStack_00023

Content:

Service name:	Csm_SignatureGenerateCsm_SignatureGenerate	
Syntax:	Std_ReturnType Csm_SignatureGenerate(uint32 jobId, Crypto_OperationModeType mode, const uint8* dataPtr, uint32 dataLength, uint8* resultPtr, uint32* resultLengthPtr)	
Service ID[hex]:	0x76	
Sync/Async:	Sync or Async, dependend on the job configuration	
Reentrancy:	Reentrant	
Parameters (in):	jobIdCsm_SignatureGenerate.jobId	Holds the identifier of the job using the CSM service.
	modeCsm_SignatureGenerate.mode	The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way: Indicates which operation mode(s) to perform.
	dataPtrCsm_SignatureGenerate.dataPtr	Contains the pointer to the data to be signed.
	dataLengthCsm_Signature Generate.dataLength	Contains the number of bytes to sign.
Parameters (inout):	resultLengthPtrCsm_Signature Generate.resultLengthPtr	Contains the number of Holds a pointer to the memory location in which the output length in bytes of the associated datasignature 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.
Parameters (out):	resultPtrCsm_SignatureGenerate.result Ptr	Contains the pointer to the data where the signature shall be stored.
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CRYPTO_E_BUSY: request failed, service is still busy CRYPTO_E_QUEUE_FULL: request failed, the queue is full CRYPTO_E_KEY_NOT_VALID: request failed, the key's state is "invalid" CRYPTO_E_SMALL_BUFFER: the provided buffer is too small to store the result.
Description:	Uses the given data to perform the signature calculation and stores the signature in the memory location pointed by the result 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 perfom."
[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]: 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 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

1.71 Specification Item SWS_Csm_00993

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = dataPtr,

job->jobPrimitiveInputOutput.inputLength = dataLength,

job->jobPrimitiveInputOutput.outputPtr = resultPtr,

job->jobPrimitiveInputOutput.outputLengthPtr = resultLengthPtr,

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
The CSM specification is described as below:

1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

However, there are no definition of following three CRYIF intefaces in CRYIF specification:

1. CryIf_SecureCounterIncrement
2. CryIf_SecureCounterRead
3. CryIf_RandomGenerate

Could you please check and solve it?

Agreed solution:

[SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

add note to 7.2.2.2.1 after [SWS_Csm_00939]:
Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]

[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.72 Specification Item SWS_Csm_00996

Trace References:

SRS_CryptoStack_00023

Content:

Service name:	Csm_SignatureVerifyCsm_SignatureVerify
Syntax:	Std_ReturnType Csm_SignatureVerify(uint32 jobId, Crypto_OperationModeType mode, const uint8* dataPtr, uint32 dataLength, const uint8* singaturesignaturePtr, uint32 signatureLength, Crypto_VerifyResultType* verifyPtr)
Service ID[hex]:	0x64
Sync/Async:	Sync or Async, dependend on the job configuration

Reentrancy:	Reentrant	
Parameters (in):	jobIdCsm_SignatureVerify.jobId	Holds the identifier of the job using the CSM service.
	modeCsm_SignatureVerify.mode	The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way:
	dataPtrCsm_SignatureVerify.dataPtr	Contains the pointer to the data to be verified.
	dataLengthCsm_SignatureVerify.dataLength	Contains the number of data bytes.
	singaturesignaturePtrCsm_SignatureVerify.singaturesignaturePtr	Holds a pointer to the signature to be verified.
	signatureLengthCsm_SignatureVerify.signatureLength	Contains the signature length in bytes.
Parameters (inout):	None	
Parameters (out):	verifyPtrCsm_SignatureVerify.verifyPtr	Holds a pointer to the memory location, which will hold the result of the signature verification.
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CRYPTO_E_BUSY: request failed, service is still busy CRYPTO_E_QUEUE_FULL: request failed, the queue is full CRYPTO_E_KEY_NOT_VALID: request failed, the key's state is "invalid" CRYPTO_E_SMALL_BUFFER: the provided buffer is too small to store the result.
Description:	Verifies the given MAC by comparing if the signature is generated with the given data.	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77724: [CRYPTO] typo in SWS_Csm_00996/Csm_SignatureVerify

  Problem description:

  In SWS_Csm_00996/Csm_SignatureVerify there is a typo in parameter "singaturePtr" (switched g and n). It should be "signaturePtr".

  Agreed solution:

  SWS_Csm_00996:

  In Syntax and Parameters(in) replace "singaturePtr" with "signaturePtr"
  –Last change on issue 77724 comment 2–

  BW-C-Level:

Application	Specification	Bus
1	3	1

1.73 Specification Item SWS_Csm_00997

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = dataPtr,

job->jobPrimitiveInputOutput.inputLength = dataLength,

job->jobPrimitiveInputOutput.secondaryInputPtr = signaturePtr,

job->jobPrimitiveInputOutput.secondaryInputLength = signatureLength,

job->jobPrimitiveInputOutput.verifyPtr = verifyPtr.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead
  3. CryIf_RandomGenerate

  Could you please check and solve it?

Agreed solution:

[SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

add note to 7.2.2.2.1 after [SWS_Csm_00939]:
Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr

generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.74 Specification Item SWS_Csm_01000

Trace References:

none

Content:

If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead(). The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_SecureCounterRead() and shall be filled in the following way:

job->jobPrimitiveInputOutput.output64Ptr = counterValuePtr

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead

3. CryIf_RandomGenerate

Could you please check and solve it?

Agreed solution:

[SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

add note to 7.2.2.2.1 after [SWS_Csm_00939]:
Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):

step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.75 Specification Item SWS_Csm_01001

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate() and shall be set in the following way:

job->jobPrimitiveInputOutput.outputPtr = resultPtr,

job->jobPrimitiveInputOutput.outputLengthPtr = resultLengthPtr.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement

2. CryIf_SecureCounterRead
3. CryIf_RandomGenerate

Could you please check and solve it?

Agreed solution:

[SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

add note to 7.2.2.2.1 after [SWS_Csm_00939]:
Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.76 Specification Item SWS_Csm_01008

Trace References:

none

Content:

Name	Crypto_AlgorithmInfoTypeCrypto_AlgorithmInfoType		
Kind	Structure		
Elements	familyCrypto_AlgorithmInfo Type.family	Crypto_AlgorithmFamilyType	The family of the algorithm
	secondaryFamily Crypto_AlgorithmInfo Type.secondaryFamily	Crypto_AlgorithmFamilyType	The operation mode to be used with that secondary family of the algorithm
	keyLengthCrypto_Algorithm InfoType.keyLength	uint32	The key length in bits to be used with that algorithm
	modeCrypto_AlgorithmInfo Type.mode	Crypto_AlgorithmModeType	The secondary family of the operation mode to be used with that algorithm
Description	Structure which determines the exact algorithm. Note, not every algorithm needs to specify all fields. AUTOSAR shall only allow valid combinations.		
Variation	–		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76985: [CRYPTO] incorrect specification of Crypto_AlgorithmInfoType

  Problem description:

  In SWS_Csm_01008 the elements "secondaryFamily" and "mode" are not correctly specified.
  It seems that the description of the one element is swapped with the description of the other element.

  Agreed solution:

[SWS_Csm_01008]: change to this:
secondaryFamily Crypto_AlgorithmFamilyType The secondary family of the algorithm
mode Crypto_AlgorithmModeType The operation mode to be used with that algorithm
–Last change on issue 76985 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.77 Specification Item SWS_Csm_01009

Trace References:

none

Content:

Name	Crypto_JobPrimitiveInputOutputTypeCrypto_JobPrimitiveInputOutputType
Kind	Structure

Name	Crypto_JobPrimitiveInputOutputTypeCrypto_JobPrimitiveInputOutputType		
Elements	inputPtrCrypto_JobPrimitiveInputOutputType.inputPtr	const uint8*	Pointer to the input data.
	inputLengthCrypto_JobPrimitiveInputOutputType.inputLength	Crypto_AlgorithmModeType uint32	Contains the input length in bytes.
	secondaryInputPtrCrypto_JobPrimitiveInputOutputType.secondaryInputPtr	const uint8*	Pointer to the secondary input data (for MacVerify, SignatureVerify).
	secondaryInputLengthCrypto_JobPrimitiveInputOutputType.secondaryInputLength	uint32	Contains the secondary input length in bytes.
	tertiaryInputPtrCrypto_JobPrimitiveInputOutputType.tertiaryInputPtr	const uint8*	Pointer to the tertiary input data (for MacVerify, SignatureVerify).
	tertiaryInputLengthCrypto_JobPrimitiveInputOutputType.tertiaryInputLength	uint32	Contains the tertiary input length in bytes.
	outputPtrCrypto_JobPrimitiveInputOutputType.outputPtr	uint8*	Pointer to the output data.
	outputLengthPtrCrypto_JobPrimitiveInputOutputType.outputLengthPtr	uint32*	Holds a pointer to a memory location containing the output length in bytes.
	secondaryOutputPtrCrypto_JobPrimitiveInputOutputType.secondaryOutputPtr	uint8*	Pointer to the secondary output data.
	secondaryOutputLengthPtrCrypto_JobPrimitiveInputOutputType.secondaryOutputLengthPtr	uint32*	Holds a pointer to a memory location containing the secondary output length in bytes.
	input64Crypto_JobPrimitiveInputOutputType.input64	uint64	versatile input parameter
	verifyPtrCrypto_JobPrimitiveInputOutputType.verifyPtr	Crypto_VerifyResultType*	Output pointer to a memory location holding a Crypto_VerifyResultType
	output64PtrCrypto_JobPrimitiveInputOutputType.output64Ptr	uint64*	Output pointer to a memory location holding an a uint64.
	modeCrypto_JobPrimitiveInputOutputType.mode	Crypto_OperationModeType	Indicator of the mode(s)/operation(s) to be performed
Description	Structure which contains input and output information depending on the job and the crypto primitive.		
Variation	–		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #74087: Change "an uint" to "a uint"

Problem description:

Remainder from # 73404:
The affected documents contain text generated artefacts which contain the text "an uint".

Correct is "a uint".

The changes of the artefacts need changes in Metamodel and BSW UML Model.

Agreed solution:

Change "an uint" to "a uint" in metamodel artifacts.
–Last change on issue 74087 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead
  3. CryIf_RandomGenerate

  Could you please check and solve it?

  Agreed solution:

[SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

add note to 7.2.2.2.1 after [SWS_Csm_00939]:
Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

- RfC #77110: [CRYPTO] wrong type for Crypto_JobPrimitiveInputOutputType.inputLength

  Problem description:

  The type of member 'inputLength' of 'Crypto_JobPrimitiveInputOutputType' ([SWS_Csm_01009]) is specified to 'Crypto_AlgorithmModeType'.
  It type of the member shall be 'uint32' instead.

  Agreed solution:

  In [SWS_Csm_01009]:

  Change the type of 'inputLength' from 'Crypto_AlgorithmModeType' to 'uint32'.
  –Last change on issue 77110 comment 2–

  BW-C-Level:

Application	Specification	Bus
4	4	1

- RfC #77261: [CRYPTO] "inputPtr" in "Crypto_JobPrimitiveInputOutputType" shall be "const uint8*"

  Problem description:

  In [SWS_Csm_01009] the element "inputPtr" of structure "Crypto_JobPrimitiveInputOutputType" is specified to "uint8*". But it shall be "const uint8*".

  Agreed solution:

  [SWS_Csm_01009]
  change type of "inputPtr" to "const uint8*".
  –Last change on issue 77261 comment 2–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.78 Specification Item SWS_Csm_01012

Trace References:

SRS_CryptoStack_00008

Content:

Name	Crypto_JobPrimitiveInfoTypeCrypto_JobPrimitiveInfoType		
Kind	Structure		
Elements	callbackIdCrypto_JobPrimitiveInfoType.callbackId	const uint32	Identifier of the callback function, to be called, if the configured service finished.
	primitiveInfoCrypto_JobPrimitiveInfoType.primitiveInfo	const Crypto_PrimitiveInfoType*	Pointer to a structure containing further configuration of the crypto primitives
	secureCounterIdCrypto_JobPrimitiveInfoType.secureCounterId	const uint32	Identifier of a secure counter.
	cryIfKeyIdCrypto_JobPrimitiveInfoType.cryIfKeyId	const uint32	Identifier of the CryIf key.
	processingTypeCrypto_JobPrimitiveInfoType.processingType	const boolean Crypto_ProcessingType	Determines the synchronous or asynchronous behavior.
	callbackUpdateNotificationCrypto_JobPrimitiveInfoType.callbackUpdateNotification	const Crypto_ProcessingType boolean	Indicates, whether the callback function shall be called, if the UPDATE operation has finished.
Description	Structure which contains further information, which depends on the job and the crypto primitive.		
Variation	–		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76983: [CRYPTO] incorrect specification of Crypto_JobPrimitiveInfoType

  Problem description:

  In SWS_Csm_01012 the elements "processingType" and "callbackUpdateNotification" are not correctly specified.
  It seems that the data type specification of the one element is swapped with the data type specification of the other element.

  Agreed solution:

  [SWS_Csm_01012]:
  change:
  processingType const Crypto_ProcessingType Determines the synchronous or asynchronous behavior.
  callbackUpdateNotification const boolean Indicates, whether the callback function shall be called, if the UPDATE operation has finished.
  –Last change on issue 76983 comment 2–

  BW-C-Level:

Application	Specification	Bus
4	4	1

1.79 Specification Item SWS_Csm_01013

Trace References:

none

Content:

Name	Crypto_JobTypeCrypto_JobType		
Kind	Structure		
Elements	jobIdCrypto_JobType.jobId	const uint32	Identifier for the job structure.
	statejobStateCrypto_Job Type.state jobState	Crypto_JobStateType	Determines the current job state.
	jobPrimitiveInputOutput Crypto_JobType.jobPrimitive InputOutput	Crypto_JobPrimitiveInput OutputType	Structure containing input and output information depending on the job and the crypto primitive.
	jobPrimitiveInfoCrypto_Job Type.jobPrimitiveInfo	const Crypto_JobPrimitive InfoType*	Pointer to a structure containing further information, which depends on the job and the crypto primitive
	jobInfoCrypto_JobType.job Info	const Crypto_JobInfoType*	Pointer to a structure containing further information, which depends on the job and the crypto primitive
	cryptoKeyIdCrypto_Job Type.cryptoKeyId	uint32	Identifier of the Crypto Driver key. The identifier shall be written by the Crypto Interface
Description	Structure which contains further information, which depends on the job and the crypto primitive.		
Variation	–		

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 perfom."
[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]: 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

1.80 Specification Item SWS_Csm_01015

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = dataPtr,

job->jobPrimitiveInputOutput.inputLength = dataLength,

job->jobPrimitiveInputOutput.outputPtr = resultPtr,

job->jobPrimitiveInputOutput.outputLengthPtr = resultLengthPtr.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId

shall be used as parameter in CryIf_RandomGenerate()...

However, there are no definition of following three CRYIF intefaces in CRYIF specification:

1. CryIf_SecureCounterIncrement
2. CryIf_SecureCounterRead
3. CryIf_RandomGenerate

Could you please check and solve it?

Agreed solution:

[SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

add note to 7.2.2.2.1 after [SWS_Csm_00939]:
Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr

SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.81 Specification Item SWS_Csm_01016

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = dataPtr,

job->jobPrimitiveInputOutput.inputLength = dataLength,

job->jobPrimitiveInputOutput.secondaryInputPtr = macPtr,

job->jobPrimitiveInputOutput.secondaryInputLength = macLength,

job->jobPrimitiveInputOutput.verifyPtr = verifyPtr.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).

The CSM specification is described as below:

1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

However, there are no definition of following three CRYIF intefaces in CRYIF specification:

1. CryIf_SecureCounterIncrement
2. CryIf_SecureCounterRead
3. CryIf_RandomGenerate

Could you please check and solve it?

Agreed solution:

[SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

add note to 7.2.2.2.1 after [SWS_Csm_00939]:
Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

remove the following requirements:
[SWS_Csm_01015]
[SWS_Csm_01017]
[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]

[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	**Specification**	**Bus**
4	4	1

1.82 Specification Item SWS_Csm_01017

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = dataPtr,

job->jobPrimitiveInputOutput.inputLength = dataLength,

job->jobPrimitiveInputOutput.outputPtr = resultPtr,

job->jobPrimitiveInputOutput.outputLengthPtr = resultLengthPtr,

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead
  3. CryIf_RandomGenerate

  Could you please check and solve it?

  Agreed solution:

  [SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

  add note to 7.2.2.2.1 after [SWS_Csm_00939]:
  Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

  remove the following requirements:
  [SWS_Csm_01015]
  [SWS_Csm_01017]
  [SWS_Csm_01016]
  [SWS_Csm_00986]
  [SWS_Csm_00990]
  [SWS_Csm_01025]

[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.83 Specification Item SWS_Csm_01022

Trace References:

none

Content:

Crypto Service:	key element:	key element Name:	key element ID:	Mandatory:
MAC	Key Material	CRYPTO_KE_MAC_KEY	1	x
	Proof (SHE)	CRYPTO_KE_MAC_PROOF	2	
Signature	Key Material	CRYPTO_KE_SIGNATURE_KEY	1	x

Crypto Service:	key element:	key element Name:	key element ID:	Mandatory:
Random	Seed State	CRYPTO_KE_RANDOM_SEED_STATE	3	
	Algorithm	CRYPTO_KE_RANDOM_ALGORITHM	4	
Cipher/AEAD	Key Material	CRYPTO_KE_CIPHER_KEY	1	x
	Init Vector	CRYPTO_KE_CIPHER_IV	5	
	Proof (SHE)	CRYPTO_KE_CIPHER_PROOF	6	
	2nd Key Material	CRYPTO_KE_CIPHER_2NDKEY	7	
Key Exchange	Base	CRYPTO_KE_KEYEXCHANGE_BASE	8	x
	Private Key	CRYPTO_KE_KEYEXCHANGE_PRIVKEY	9	x
	Own Public Key	CRYPTO_KE_KEYEXCHANGE_OWNPUBKEY	10	x
	Shared Value	CYRPTO_KE_KEYEXCHANGE_SHAREDVALUE	1	x
	Algorithm	CRYPTO_KE_KEYEXCHANGE_ALGORITHM	12	
Key Derivation	Password	CRYPTO_KE_KEYDERIVATION_PASSWORD	1	x
	Salt	CRYPTO_KE_KEYDERIVATION_SALT	13	
	Iterations	CRYPTO_KE_KEYDERIVATION_ITERATIONS	14	
	Algorithm	CRYPTO_KE_KEYDERIVATION_ALGORITHM	15	
Key Generate	Key Material	CRYPTO_KE_KEYGENERATE_KEY	1	x
	Seed	CRYPTO_KE_KEYGENERATE_SEED	16	
	Algorithm	CRYPTO_KE_KEYGENERATE_ALGORITHM	17	

Crypto Service:	key element:	key element Name:	key element ID:	Mandatory:
Certificate Parsing	Certificate	CRYPTO_KE_CERTIFICATE_DATA	0	x
	Format	CRYPTO_KE_CERTIFICATE_PARSING_FORMAT	18	
	Current Time	CRYPTO_KE_CERTIFICATE_CURRENT_TIME	19	
	Version	CRYPTO_KE_CERTIFICATE_VERSION	20	
	Serial Number	CRYPTO_KE_CERTIFICATE_SERIALNUMBER	21	
	Signature Algroithm	CRYPTO_KE_CERTIFICATE_SIGNATURE_ALGORITHM	22	
	Issuer	CRYPTO_KE_CERTIFICATE_ISSUER	23	
	Validity start	CRYPTO_KE_CERTIFICATE_VALIDITY_NOT_BEFORE	24	
	Validity end	CRYPTO_KE_CERTIFICATE_VALIDITY_NOT_AFTER	25	
	Subject	CRYPTO_KE_CERTIFICATE_SUBJECT	26	
	Subject Public Key	CRYPTO_KE_CERTIFICATE_SUBJECT_PUBLIC_KEY	1	
	Extensions	CRYPTO_KE_CERTIFICATE_EXTENSIONS	27	
	Signature	CRYPTO_KE_CERTIFICATE_SIGNATURE	28	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76782: [CRYPTO] Missing Information about SWS_Crypto_00044

  Problem description:

  According to [SWS_Crypto_00037], the index of the key elements are defined in imported types table [SWS_Crypto_00044].
  However, there is no description about [SWS_Crypto_00044] in CRYPTO specification.

  The following description may apply to [SWS_Crypto_00044], but the description is broken.

  The Crypto Stack API uses the key element index definition from the CSM

module.
Type definitions
N/A.

Could you please check and adjust it?

Agreed solution:

CryptoDriver:
- SWS_Crypto_00037: Replace SWS_Crypto_00044 by SWS_Csm_01022

CSM
- SWS_Csm_01022: Correct the tag by moving it out of the table
–Last change on issue 76782 comment 10–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.84 Specification Item SWS_Csm_01023

Trace References:

none

Content:

Service name:	Csm_AEADEncryptCsm_AEADEncrypt
Syntax:	Std_ReturnType Csm_AEADEncrypt(uint32 jobId, Crypto_OperationModeType mode, const uint8* plaintextPtr, uint32 plaintextLength, const uint8* associatedDataPtr, uint32 associtatedassociatedDataLengthPtr, uint8* ciphertextPtr, uint32* ciphertextLengthPtr, uint8* tagPtr, uint32* tagLengthPtr)
Service ID[hex]:	0x62
Sync/Async:	Sync or Async, dependend on the job configuration
Reentrancy:	Reentrant

Parameters (in):	jobIdCsm_AEADEncrypt.jobId	Holds the identifier of the job using the CSM service.
	modeCsm_AEADEncrypt.mode	Indicates which operation mode(s) to perfom.
	plaintextPtrCsm_AEADEncrypt.plaintextPtr	Contains the pointer to the data to be encrypted.
	plaintextLength Csm_AEADEncrypt.plaintextLength	Holds a pointer to the memory location in which the output length in bytes of the paintext is stored. On calling this function, this parameter shall contain the size of the buffer provided by plaintextPtr. When the request has finished, the actual length of the returned value shall be stored. Contains the number of bytes to encrypt.
	associatedDataPtr Csm_AEADEncrypt.associatedDataPtr	Contains the pointer to the associated data.
	associtatedassociatedDataLengthPtr Csm_AEADEncrypt.associtatedassociatedDataLength Ptr	Contains the number of bytes of the associated data.
Parameters (inout):	ciphertextLengthPtr Csm_AEADEncrypt.ciphertextLengthPtr	Holds a pointer to the memory location in which the output length in bytes of the ciphertext is stored. On calling this function, this parameter shall contain the size of the buffer in bytes provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored.
	tagLengthPtrCsm_AEADEncrypt.tagLengthPtr	Holds a pointer to the memory location in which the output length in bytes of the Tag is stored. On calling this function, this parameter shall contain the size of the buffer in bytes provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored.
Parameters (out):	ciphertextPtr Csm_AEADEncrypt.ciphertextPtr	Contains the pointer to the data where the encrypted data shall be stored.
	tagPtrCsm_AEADEncrypt.tagPtr	Contains the pointer to the data where the Tag shall be stored.
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CRYPTO_E_BUSY: request failed, service is still busy CRYPTO_E_QUEUE_FULL: request failed, the queue is full CRYPTO_E_KEY_NOT_VALID: request failed, the key's state is "invalid"
Description:	Uses the given input data to perform a AEAD encryption and stores the ciphertext and the MAC in the memory locations pointed by the ciphertext pointer and Tag 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 perfom."
[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]: 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

1.85 Specification Item SWS_Csm_01025

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = plaintextPtr,

job->jobPrimitiveInputOutput.inputLength = plaintextLength,

job->jobPrimitiveInputOutput.secondaryInputPtr = associatedDataPtr,

job->jobPrimitiveInputOutput.secondaryInputLength = associatedDataLengthPtr,

job->jobPrimitiveInputOutput.outputPtr = ciphertextPtr,

job->jobPrimitiveInputOutput.outputLength = ciphertextLength,

job->jobPrimitiveInputOutput.secondaryOutputPtr = tagPtr,

job->jobPrimitiveInputOutput.secondaryOutputLengthPtr = tagLengthPtr.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead
  3. CryIf_RandomGenerate

  Could you please check and solve it?

  Agreed solution:

  [SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

  add note to 7.2.2.2.1 after [SWS_Csm_00939]:
  Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

  remove the following requirements:
  [SWS_Csm_01015]
  [SWS_Csm_01017]
  [SWS_Csm_01016]
  [SWS_Csm_00986]
  [SWS_Csm_00990]
  [SWS_Csm_01025]

[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.86 Specification Item SWS_Csm_01026

Trace References:

none

Content:

Service name:	Csm_AEADDecryptCsm_AEADDecrypt

Syntax:	Std_ReturnType Csm_AEADDecrypt(uint32 jobId, Crypto_OperationModeType mode, const uint8* ciphertextPtr, uint32 ciphertextLength, const uint8* associatedDataPtr, uint32 associtatedassociatedDataLength, const uint8* tagPtr, uint32 tagLength, uint8* plaintextPtr, uint32* plaintextLengthPtr, Crypto_VerifyResultType* verifyPtr)	
Service ID[hex]:	0x63	
Sync/Async:	Sync or Async, dependend on the job configuration	
Reentrancy:	Reentrant	
Parameters (in):	jobIdCsm_AEADDecrypt.jobId	Holds the identifier of the job using the CSM service.
	modeCsm_AEADDecrypt.mode	Indicates which operation mode(s) to perfom.
	ciphertextPtr Csm_AEADDecrypt.ciphertextPtr	Contains the pointer to the data to be decrypted.
	ciphertextLength Csm_AEADDecrypt.ciphertextLength	Contains the number of bytes to decrypt.
	associatedDataPtr Csm_AEADDecrypt.associatedDataPtr	Contains the pointer to the associated data.
	associtatedassociatedDataLength Csm_AEADDecrypt.associtatedassociatec DataLength	Contains the length in bytes of the associated data.
	tagPtrCsm_AEADDecrypt.tagPtr	Contains the pointer to the Tag to be verified.
	tagLengthCsm_AEADDecrypt.tagLength	Contains the length in bytes of the Tag to be verified.
Parameters (inout):	plaintextLengthPtr Csm_AEADDecrypt.plaintextLengthPtr	Holds a pointer to the memory location in which the output length in bytes of the paintext is stored. On calling this function, this parameter shall contain the size of the buffer provided by plaintext Ptr. When the request has finished, the actual length of the returned value shall be stored.
Parameters (out):	plaintextPtrCsm_AEADDecrypt.plaintext Ptr	Contains the pointer to the data where the decrypted data shall be stored.
	verifyPtrCsm_AEADDecrypt.verifyPtr	Contains the pointer to the result of the verification.
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CRYPTO_E_BUSY: request failed, service is still busy CRYPTO_E_QUEUE_FULL: request failed, the queue is full CRYPTO_E_KEY_NOT_VALID: request failed, the key's state is "invalid"
Description:	Uses the given data to perform an AEAD encryption and stores the ciphertext and the MAC in the memory locations pointed by the ciphertext pointer and Tag 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 perfom."
[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]: 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 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

1.87 Specification Item SWS_Csm_01027

Trace References:

none

Content:

The Crypto_JobInfoType job with the corresponding jobId shall be set in the following way:

job->jobPrimitiveInputOutput.mode = mode,

job->jobPrimitiveInputOutput.inputPtr = ciphertextPtr,

job->jobPrimitiveInputOutput.inputLength = ciphertextLength,

job->jobPrimitiveInputOutput.secondaryInputPtr = associatedDataPtr,

job->jobPrimitiveInputOutput.secondaryInputLength = associatedLength,

job->jobPrimitiveInputOutput.tertiaryInputPtr = tagPtr,

job->jobPrimitiveInputOutput.tertiaryInputLength = tagLength,

job->jobPrimitiveInputOutput.outputPtr = plaintextPtr, job->jobPrimitiveInputOutput.outputLengthPtr = plaintextLengthPtr.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76745: Missing three CRYIF Interfaces

  Problem description:

  There are no three CRYIF interfaces which are provided for Crypto Service Manager(CSM).
  The CSM specification is described as below:

  1. [SWS_Csm_00973] If no errors are detected by Csm, the service Csm_SecureCounterIncrement() shall call CryIf_SecureCounterIncrement().
  2. [SWS_Csm_01000] If no errors are detected by Csm, the service Csm_SecureCounterRead() shall call CryIf_SecureCounterRead().
  3. [SWS_Csm_01001] The Crypto_JobInfoType job with the corresponding jobId shall be used as parameter in CryIf_RandomGenerate()...

  However, there are no definition of following three CRYIF intefaces in CRYIF specification:

  1. CryIf_SecureCounterIncrement
  2. CryIf_SecureCounterRead
  3. CryIf_RandomGenerate

  Could you please check and solve it?

  Agreed solution:

  [SWS_Csm_01009]: Add additional element (after verifyPtr): "input64 uint64 versatile input parameter"

  add note to 7.2.2.2.1 after [SWS_Csm_00939]:
  Note: The Csm_<Service>() will call the CryIf_ProcessJob() with a pointer to Crypto_JobType, where all the necessary information are stored to process the job. Part of this Crypto_JobType is a Crypto_JobPrimitiveInputOutputType, where all the information about the input and output parameters depending of the service are stored. A definition of the mapping from the API parameters of Csm_<Service>() to the parameters of Crypto_JobPrimitiveInputOutputType, can be found in [SWS_Crypto_00073] of the Crypto Driver specification.

  remove the following requirements:
  [SWS_Csm_01015]
  [SWS_Csm_01017]

[SWS_Csm_01016]
[SWS_Csm_00986]
[SWS_Csm_00990]
[SWS_Csm_01025]
[SWS_Csm_01027]
[SWS_Csm_00993]
[SWS_Csm_00997]
[SWS_Csm_00973]
[SWS_Csm_01000]
[SWS_Csm_01001]

[SWS_Crypto_00073]:
Add to the table the following rows and columns (input64 and output64Ptr are new columns)

Service: Output input64 output64Ptr
SECURECOUNTERINCREMENT step size

SECURECOUNTERREAD value of counter

RANDOMGENERATE generated random

for clarification (Tabulator are not precise enough):
step size should be in column input64
value of counter should be in column output64Ptr
generated random should be in column Output
–Last change on issue 76745 comment 20–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.88 Specification Item SWS_Csm_01029

Trace References:

none

Content:

Name	Crypto_OperationModeTypeCrypto_OperationModeType
Kind	Enumeration

Name	Crypto_OperationModeTypeCrypto_OperationModeType		
Range	CRYPTO_OPERATIONMODE_STARTCrypto_OperationModeType.CRYPTO_OPERATIONMODE_START	0x01	Operation Mode is "Start". The job's state shall be reset, i.e. previous input data and intermediate results shall be deleted.
	CRYPTO_OPERATIONMODE_UPDATECrypto_OperationModeType.CRYPTO_OPERATIONMODE_UPDATE	0x02	Operation Mode is "Update". Used to calculate intermediate results.
	CRYPTO_OPERATIONMODE_STREAMSTARTCrypto_OperationModeType.CRYPTO_OPERATIONMODE_STREAMSTART	0x03	Operation Mode is "Stream Start". Mixture of "Start" and "Update". Used for streaming.
	CRYPTO_OPERATIONMODE_FINISHCrypto_OperationModeType.CRYPTO_OPERATIONMODE_FINISH	0x04	Operation Mode is "Finish". The calculations shall be finalized.
	CRYPTO_OPERATIONMODE_SINGLECALLCrypto_OperationModeType.CRYPTO_OPERATIONMODE_SINGLECALL	0x05 0x07	Operation Mode is "Single Call". Mixture of "Start", "Update" and "Finish".
Description	– Enumeration which operation shall be performed. This enumeration is constructed from a bit mask, where the first bit indicates "Start", the second "Update" and the third "Finish".		
Variation	–		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76930: [CRYPTO] Crypto_OperationModeType is not specified

  Problem description:

  Data type 'Crypto_OperationModeType' is used in new API interfaces, but is specified nowhere in the document.

  Agreed solution:

  Include the specification of 'Crypto_OperationModeType' into the release document, as it was contained in the draft documents.

  It should be included to Chapter 8.7.2 "Implementation Data Types" as Chapter 8.7.2.3 "Crypto_OperationModeType" (all following Implementation Data Types should be moved one downwards).

  [SWS_Csm_01029]
  Name: Crypto_OperationModeType
  Kind: Enumeration
  Range: CRYPTO_OPERATIONMODE_START 1 Operation Mode is Start. The job's state shall be reset, i.e. previous input data and intermediate results shall be deleted.
  CRYPTO_OPERATIONMODE_UPDATE 2 Operation Mode is Update. Used to

calculate intermediate results.
CRYPTO_OPERATIONMODE_STREAMSTART 3 Operation Mode is Stream Start. Mixture of Start and Update. Used for streaming.
CRYPTO_OPERATIONMODE_FINISH 4 Operation Mode is Finish. The calculations shall be finalized.
CRYPTO_OPERATIONMODE_SINGLECALL 7 Operation Mode is Single Call. Mixture of Start, Update and Finish.
Description: Enumeration which operation shall be performed. This enumeration is constructed from a bit mask, where the first bit indicates Start, the second Update and the third Finish.
–Last change on issue 76930 comment 9–

BW-C-Level:

Application	Specification	Bus
1	4	1

1.89 Specification Item SWS_Csm_01031

Trace References:

none

Content:

Name	Crypto_ServiceInfoTypeCrypto_ServiceInfoType
Kind	Enumeration

Name	Crypto_ServiceInfoTypeCrypto_ServiceInfoType		
Range	CRYPTO_HASHCrypto_Service InfoType.CRYPTO_HASH	0x00	Hash Service
	CRYPTO_MACGENERATECrypto_Service Info Type.CRYPTO_MACGENERATE	0x01	MacGenerate Service
	CRYPTO_MACVERIFYCrypto_Service Info Type.CRYPTO_MACVERIFY	0x02	MacVerify Service
	CRYPTO_ENCRYPTCrypto_Service Info Type.CRYPTO_ENCRYPT	0x03	Encrypt Service
	CRYPTO_DECRYPTCrypto_Service Info Type.CRYPTO_DECRYPT	0x04	Decrypt Service
	CRYTPOCRYPTO_AEADENCRYPTCrypto_Service Info Type.CRYTPOCRYPTO_AEADENCRYPT	0x05	AEADEncrypt Service
	CRYPTO_AEADDECRYPTCrypto_Service Info Type.CRYPTO_AEADDECRYPT	0x06	AEADDecrypt Service
	CRYPTO_SIGNATUREGENERATECrypto_Service Info Type.CRYPTO_SIGNATUREGENERATE	0x07	SignatureGenerate Service
	CRYPTO_SIGNATUREVERIFYCrypto_Service Info Type.CRYPTO_SIGNATUREVERIFY	0x08	SignatureVerify Service
	CRYPTO_SECCOUNTERINCREMENTCrypto_Service Info Type.CRYPTO_SECCOUNTERINCREMENT	0x09	SecureCounterIncrement Service
	CRYPTO_SECCOUNTERREADCrypto_Service Info Type.CRYPTO_SECCOUNTERREAD	0x0A	SecureCounterDecrement Read Service
	CRYPTO_RANDOMGENERATECrypto_Service Info Type.CRYPTO_RANDOMGENERATE	0x0B	RandomGenerate Service
Description	Enumeration of the kind of the service.		
Variation	–		

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 perfom."
[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]: 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 #77722: [CRYPTO] typo in SWS_Csm_01031/Crypto_ServiceInfoType

  Problem description:

  In SWS_Csm_01031/Crypto_ServiceInfoType the value CRYTPO_AEADENCRYPT shall be CRYPTO_AEADENCRYPT ... switch T and P in CRYPTO.

  Agreed solution:

  in SWS_Csm_01031:

  replace CRYTPO_AEADENCRYPT with CRYPTO_AEADENCRYPT
  –Last change on issue 77722 comment 3–

  BW-C-Level:

Application	Specification	Bus
4	4	1

1.90 Specification Item SWS_Csm_01035

Trace References:

none

Content:

If no errors are detected by Csm and the keyId and targetKeyId are located in the same Crypto Driver, the service Csm_KeyCopy() shall call CryIf_KeyElementCopy()and pass on the return value.

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 perfom."
[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]: 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

1.91 Specification Item SWS_Csm_01044

Trace References:

none

Content:

If the CRYPTO_OPERATIONMODE_FINISH bit is set in job->jobPrimitiveInputOutput.mode, the Csm_CallbackFunction Notification shall call the configured callback function.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76982: [CRYPTO] unspecified identifier Csm_CallbackFunction

  Problem description:

  Requirements SWS_Csm_01053 and SWS_Csm_01044 refering to an identifier "Csm_CallbackFunction" that is not specified in the document.

  Agreed solution:

  In [SWS_Csm_01053] and [SWS_Csm_01044]: replace "Csm_CallbackFunction" with "Csm_CallbackNotification"
  –Last change on issue 76982 comment 2–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.92 Specification Item SWS_Csm_01053

Trace References:

none

Content:

If the CRYPTO_OPERATIONMODE_UPDATE bit is set in job-> jobPrimitiveInputOutput.mode and the corresponding CsmJobPrimitiveCallbackUpdateNotification (ECUC_CSM_00064Csm_00124) is true, the Csm_CallbackFunction Notification shall call the configured callback function.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76982: [CRYPTO] unspecified identifier Csm_CallbackFunction

  Problem description:

  Requirements SWS_Csm_01053 and SWS_Csm_01044 refering to an identifier "Csm_CallbackFunction" that is not specified in the document.

  Agreed solution:

  In [SWS_Csm_01053] and [SWS_Csm_01044]: replace "Csm_CallbackFunction" with "Csm_CallbackNotification"
  –Last change on issue 76982 comment 2–

  BW-C-Level:

Application	Specification	Bus
1	1	1

- RfC #77806: Clarify CsmJobPrimitiveCallbackUpdateNotification

  Problem description:

  It seems that there is a conflict between CSM, CRYIF and CRYPTO requirements regarding the callback function for operation mode UPDATE:

  [SWS_Crypto_00028] For each asynchronous request the Crypto Driver shall notify CRYIF about the completion of the job by calling the CRYIF_CallbackNotification function passing on the job information and the result of cryptographic operation.

  [SWS_Csm_01053] If the CRYPTO_OPERATIONMODE_UPDATE bit is set in job-> jobPrimitiveInputOutput.mode and the corresponding CsmJobPrimitiveCallbackUpdateNotification (ECUC_CSM_00064) is true, the Csm_CallbackFunction shall call the configured callback function.
  (By the way, it's not ECUC_CSM_00064 but ECUC_Csm_00124.)

SWS_Crypto_00028 demands to call the callback notification function independently of the completed operation. This is also supported by:

[SWS_CryIf_91013] + [SWS_CryIf_00109] If no errors are detected by CRYIF, the service CryIf_CallbackNotification() shall call Csm_CallbackNotification() and pass on the result.

But CSM limits the callback chain in case CsmJobPrimitiveCallbackUpdateNotification is false.

Shall only CSM suppress the call of the callback notification? Or shall this already be checked in CRYPTO?
What is the usecase behind
ECUC_Csm_00124?

Agreed solution:

SWS_Csm_01053: Update ECUC reference to correct one (ECUC_Csm_00124)
–Last change on issue 77806 comment 2–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.93 Specification Item SWS_Csm_01074

Trace References:

SRS_CryptoStack_00090

Content:

Name	Csm_AEADEncryptAEADDecryptMacType_{Crypto}Csm_AEADDecryptMacType		
Kind	Array	Element type	uint8
Size	{ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/CsmAEADDecryptMacLength}/8		
Description	Array long enough to store the data of the Tag.		
Variation	Crypto= {ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig.SHORT-NAME)}		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77267: [CRYPTO] wrong size specification for Csm_AEADEncryptMacType_Crypto and Csm_AEADDecryptTagType_Crypto

  Problem description:

  a)
  SWS_Csm_01926/Csm_AEADEncryptMacType_Crypto specifies the size to "ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/" elements. but it shall be "ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEADE
  bytes.

  b)
  SWS_Csm_01074/Csm_AEADDecryptTagType_Crypto specifies the size to "ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/ CsmAEADDecryptMacLength/8" elements. but it shall be "(ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/ CsmAEADDecryptMacLength/8)+1)" bytes.

  c)
  Note that the Title of the requirements is "TAGtype" whereas the name is specified to "MACtype".

  Agreed solution:

  [SWS_Csm_01926]
  Change its headline: Csm_AEADEncryptMacType_Crypto

  Change size to: ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEAD
  Elements

  [SWS_Csm_01074]
  Change its headline: Csm_AEADDecryptMacType_Crypto

  Change size to: ((ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/CsmAEA
  Elements

  [SWS_Csm_00803]
  Change size to: (ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerifyConfig/CsmMacVerifyCo
  Elements
  –Last change on issue 77267 comment 18–

  BW-C-Level:

Application	Specification	Bus
1	4	1

1.94 Specification Item SWS_Csm_01080

Trace References:

SRS_CryptoStack_00090

Content:

Name	Csm_AsymPrivateKeyTypeCsm_AsymPrivateKeyType		
Kind	Structure		
Elements	lengthCsm_AsymPrivateKeyType.length	uint32	This element contains the length of the key stored in element 'data'
	dataCsm_AsymPrivateKeyType.data	Csm_AlignAsymPrivateKeyArrayType	This element contains the key data or a key handle.
Size	CSM_ASYM_PRIV_KEY_MAX_SIZE		
Description	Structure for the private asymmetrical key. CSM_ASYM_PRIV_KEY_MAX_SIZE shall be chosen such that "CSM_ASYM_PRIV_KEY_MAX_SIZE * sizeof(Csm_AlignType)" is greater or equal to the maximum of the configured values CsmAsymDecryptMaxKeySize, CsmSignatureGenerateMaxKeySize, CsmAsymPrivateKeyExtractMaxKeySize, CsmAsymPrivateKeyWrapSymMaxPrivKeySize, CsmAsymPrivateKeyWrapAsymMaxPrivKeySize and CsmAsymPrivateKeyUpdateMaxKeySize.		
Variation	–		

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 perfom."
[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]: 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

1.95 Specification Item SWS_Csm_01543

Trace References:

SRS_CryptoStack_00019

Content:

Service name:	Csm_RandomGenerateCsm_RandomGenerate	
Syntax:	Std_ReturnType Csm_RandomGenerate(uint32 jobId, uint8* resultPtr, uint32* resultLengthPtr)	
Service ID[hex]:	0x72	
Sync/Async:	Sync or Async, dependend on the job configuration	
Reentrancy:	Reentrant	
Parameters (in):	jobIdCsm_RandomGenerate.jobId	Holds the identifier of the job using the CSM service.
Parameters (inout):	resultLengthPtrCsm_RandomGenerate.resultLengthPtr	Holds a pointer to the memory location in which the result length in bytes is stored. On calling this function, this parameter shall contain the number of random bytes, which shall be stored to the buffer provided by resultPtr. When the request has finished, the actual length of the returned value shall be stored.
Parameters (out):	resultPtrCsm_RandomGenerate.resultPtr	Holds a pointer to the memory location which will hold the result of the random number generation.
Return value:	Std_ReturnType	E_OK: request successful E_NOT_OK: request failed CRYPTO_E_BUSY: request failed, service is still busy CRYPTO_E_QUEUE_FULL: request failed, the queue is full CRYPTO_E_ENTROPY_EXHAUSTION: request failed, entropy of random number generator is exhausted.
Description:	Starts the random number generation service of the CSM module. If the service state is not "idle", the function shall return with "CRYPTO_E_BUSY". Otherwise, this function shall call CryIf_RandomGenerate()Generate a random number and stores it in the memory location pointed by the result 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 "associatedDataL-

ength"
[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 perfom."
[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]: 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

1.96 Specification Item SWS_Csm_01915

Trace References:

SRS_CryptoStack_00090

Content:

Name	CsmAEADDecrypt_{Primitive}CsmAEADDecrypt	
Comment	Interface to execute the AEAD decryption.	
IsService	true	
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecrypt Config.SHORT-NAME)}	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

AEADDecryptCsmAEADDecrypt.AEADDecrypt	
Comments	Streaming approach of the AEAD decryption.
Variation	–

AEADDecryptCsmAEADDecrypt.AEADDecrypt			
Parameters	ciphertextBufferCsm AEADDecrypt.AEADDecrypt.ciphertext Buffer	Comment	Contains the ciphertext to be decrypted with AEAD.
		Type	Csm_AEADDecrypt CiphertextType_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/Csm AEADDecrypt/Csm AEADDecrypt Config.SHORT-NAME)}
		Direction	IN
	ciphertextLengthCsm AEADDecrypt.AEADDecrypt.ciphertext Length	Comment	Contains the length in bytes of the ciphertext to be decrypted with AEAD.
		Type	uint32
		Variation	–
		Direction	IN
	associatedDataBufferCsm AEADDecrypt.AEADDecrypt.associated DataBuffer	Comment	Contains the data of the header (that is not part of the encryption but authentication) .
		Type	Csm_AEADDecrypt AssociatedData Type_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/Csm AEADDecrypt/Csm AEADDecrypt Config.SHORT-NAME)}
		Direction	IN
	associatedDataLengthCsm AEADDecrypt.AEADDecrypt.associated DataLength	Comment	Contains the length in bytes of the data of the header.
		Type	uint32
		Variation	–
		Direction	IN
	macBufferCsmAEADDecrypt.AEADDecrypt.mac Buffer	Comment	Contains the data of the MAC.
		Type	Csm_AEADEncryptAEADDecrypt MacType_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/Csm AEADDecrypt/Csm AEADDecrypt Config.SHORT-NAME)}
		Direction	IN
	macLengthCsmAEADDecrypt.AEADDecrypt.mac Length	Comment	Contains the length in BITS of the data of the MAC.
		Type	uint32
		Variation	–
		Direction	IN
	plaintextBufferCsmAEADDecrypt.AEADDecrypt.plaintext Buffer	Comment	Contains the data of the decrypted AEAD plaintext.
		Type	Csm_AEADDecryptPlaintext Type_{Crypto}
		Variation	Crypto = {ecuc(Csm/Csm Primitives/Csm AEADDecrypt/Csm

AEADDecryptCsmAEADDecrypt.AEADDecrypt		
Possible Errors	E_OK	Operation successful
	E_NOT_OK	
	CSM_E_BUSY	failed, service is still busy
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result

CancelJobCsmAEADDecrypt.CancelJob		
Comments	Cancels the job.	
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77267: [CRYPTO] wrong size specification for Csm_AEADEncryptMacType_Crypto and Csm_AEADDecryptTagType_Crypto

  Problem description:

  a)
  SWS_Csm_01926/Csm_AEADEncryptMacType_Crypto specifies the size to "ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/" elements.
  but it shall be "ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEADE
  bytes.

  b)
  SWS_Csm_01074/Csm_AEADDecryptTagType_Crypto specifies the size to "ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/
  CsmAEADDecryptMacLength/8" elements. but it shall be "(ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/
  CsmAEADDecryptMacLength/8)+1)" bytes.

  c)
  Note that the Title of the requirements is "TAGtype" whereas the name is specified to "MACtype".

  Agreed solution:

  [SWS_Csm_01926]
  Change its headline: Csm_AEADEncryptMacType_Crypto

  Change size to: ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEAD
  Elements

[SWS_Csm_01074]
Change its headline: Csm_AEADDecryptMacType_Crypto

Change size to: ((ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/CsmAE
Elements

[SWS_Csm_00803]
Change size to: (ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerifyConfig/CsmMacVerifyCo
Elements
–Last change on issue 77267 comment 18–

BW-C-Level:

Application	Specification	Bus
1	4	1

1.97 Specification Item SWS_Csm_01927

Trace References:

SRS_CryptoStack_00090

Content:

Name	Csm_AEADEncryptCiphertextType_{Crypto}Csm_AEADEncryptCiphertextType		
Kind	Array	Element type	uint8
Size	{ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmCiphertextAEADEncryptCiphertextMaxLength}		
Description	Array long enough to store the data of the cipher.		
Variation	Crypto= {ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig.SHORT-NAME)}		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77781: [CRYPTO] SWS_Csm_01927/CsmCiphertextLength

  Problem description:

  Name: Danny Block
  Phone: +49 9131 7701 6460
  Role:

SWS_Csm_01927/CsmCiphertextLength shall be CsmAEADEncryptCiphertextMaxLength.

Was there already a decision?

Agreed solution:

SWS_Csm_01927:
replace value of size:
"ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmCiphertextLength
Elements"

with

"ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEADEncryptCipher
Elements"
–Last change on issue 77781 comment 2–

BW-C-Level:

Application	Specification	Bus
4	4	1

1.98 Specification Item SWS_Csm_09000

Trace References:

SRS_CryptoStack_00090

Content:

Name	CsmMacGenerate_{Primitive}CsmMacGenerate
Comment	Interface to execute the MAC generation.
IsService	true
Variation	Primitive = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerate Config.SHORT-NAME)}

Name	CsmMacGenerate_{Primitive}CsmMacGenerate	
Possible Errors	0	E_OK
	1	E_NOT_OK
	2	CSM_E_BUSY
	3	CSM_E_SMALL_BUFFER

Operations:

CancelJobCsmMacGenerate.CancelJob		
Comments	Cancels the job.	
Variation	–	
Possible Errors	E_OK	Operation successful
	E_NOT_OK	

MacGenerateCsmMacGenerate.MacGenerate	
Comments	Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer.
Variation	–

MacGenerateCsmMacGenerate.MacGenerate			
Parameters	dataBufferCsmMacGenerate.MacGenerate.dataBuffer	Comment	Contains the length in bytes of the data from which a MAC shall be generated of.
		Type	Csm_MacGenerateDataType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig.SHORT-NAME)}
		Direction	IN
	dataLengthCsmMacGenerate.MacGenerate.dataLength	Comment	Contains the length in bytes of the data from which a MAC shall be generated of.
		Type	uint32
		Variation	–
		Direction	IN
	resultBufferCsmMacGenerate.MacGenerate.resultBuffer	Comment	Contains the data of the MAC.
		Type	Csm_MacGenerateResultType_{Crypto}
		Variation	Crypto = {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig.SHORT-NAME)}
		Direction	OUT
	resultLengthCsmMacGenerate.MacGenerate.resultLength	Comment	Contains the length in bytes of the MAC.
		Type	uint32
		Variation	–
		Direction	INOUT
Possible Errors	E_OK	Operation successful	
	E_NOT_OK		
	CSM_E_BUSY	failed, service is still busy	
	CSM_E_SMALL_BUFFER	the provided buffer is too small to store the result	

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #77264: [CRYPTO] possible errors of "CancelJob" operation of Client-Server-Interfaces

Problem description:

The specifications of the possible errors of the "CancelJob" operation of the Client-Server-Interfaces are varying.
Sometimes there is CSM_E_BUSY defined, sometimes not. Sometimes there are actually no possible errors specified.

Agreed solution:

——————————-
For 4.3.1
- Remove in every CancelJob Operation the Possible Error: "CSM_E_BUSY failed, service is still busy"
in the following Items:
[SWS_Csm_009000]
[SWS_Csm_00936]
[SWS_Csm_00947]
[SWS_Csm_00903]

- [SWS_Csm_00943]
Add Possible Errors to Operation CancelJob
Possible Errors
0 E_OK Operation successful
1 E_NOT_OK –
–Last change on issue 77264 comment 21–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.99 Specification Item SWS_Csm_91002

Trace References:

none

Content:

Name	SymBlockEncryptResultBuffer (obsolete)SymBlockEncryptResultBuffer		
Kind	Array	Element type	uint8
Description	Buffer for the output result for symmetrical block encryption. Tags: atp.Status=obsolete		

Name	SymBlockEncryptResultBuffer (obsolete)SymBlockEncryptResultBuffer
Variation	–

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_00930 -> new ID for first
  SWS_Csm_00932 -> new ID for first
  SWS_Csm_00934 -> new ID for first
  –Last change on issue 76440 comment 15–

  BW-C-Level:

Application	Specification	Bus
1	1	1

1.100 Specification Item SWS_Csm_91003

Trace References:

SRS_CryptoStack_00090, SRS_CryptoStack_00091

Content:

Name	{Job}_MacVerifyCsm.MacVerify		
Kind	ProvidedPort	Interface	CsmMacVerify_{Primitive}
Description	Port for a job to verify a MAC		
Port Defined Argument Value(s)	Type	uint32	
	Value	({ecuc(Csm/CsmJobs/CsmJob.CsmJobId)})	
	Type	Crypto_OperationModeType	
	Value	CRYPTO_OPERATIONMODE_SINGLECALL	

Variation	({ecuc(Csm/CsmJobs/CsmJob.CsmJobUsePort)} == TRUE) && ({ecuc(Csm/CsmJobs/CsmJob.CsmJobPrimitiveRef -> CsmPrimitives/CsmMacVerify)} != NULL)
	Job = {ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerifyConfig.SHORT-NAME)}
	Primitive = {ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerifyConfig.SHORT-NAME)}		

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
  SWS_Csm_00930 -> new ID for first
  SWS_Csm_00932 -> new ID for first

SWS_Csm_00934 -> new ID for first
–Last change on issue 76440 comment 15–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.101 Specification Item SWS_Csm_91004

Trace References:

SRS_CryptoStack_00086

Content:

Development Error Types

Type of error	Related error code	Value [hex]
API request called with invalid parameter (Nullpointer)	CSM_E_PARAM_POINTER	0x01
Buffer is too small for operation	CSM_E_SMALL_BUFFER	0x03
keyID is out of range	CSM_E_PARAM_HANDLE	0x04
API request called before initialization of CSM module	CSM_E_UNINIT	0x05
Initialization of CSM module failed	CSM_E_INIT_FAILED	0x07
Requested service is not initialized	CSM_E_SERVICE_NOT_STARTED	0x09

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

Agreed solution:

SWS_Csm_00037 -> new ID for second
SWS_Csm_00828 -> new ID for first
SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_00930 -> new ID for first
SWS_Csm_00932 -> new ID for first
SWS_Csm_00934 -> new ID for first
–Last change on issue 76440 comment 15–

BW-C-Level:

Application	Specification	Bus
1	1	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

1.102 Specification Item SWS_Csm_91005

Trace References:

none

Content:

Each crypto primitive configuration shall be realized as a constant structure of type Crypto_PrimitiveInfoType.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed

SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_00930 -> new ID for first
SWS_Csm_00932 -> new ID for first
SWS_Csm_00934 -> new ID for first
–Last change on issue 76440 comment 15–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.103 Specification Item SWS_Csm_91006

Trace References:

none

Content:

Each job primitive configuration shall be realized as a constant structure of type Crypto_JobPrimitiveInfoType.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected

artifact needed
SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_00930 -> new ID for first
SWS_Csm_00932 -> new ID for first
SWS_Csm_00934 -> new ID for first
–Last change on issue 76440 comment 15–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.104 Specification Item SWS_Csm_91007

Trace References:

none

Content:

If a synchronous job is issued and the priority is less than the highest priority available in the queue, the CSM shall return E_BUSY.

RfCs affecting this spec item between releases 4.3.0 and 4.3.1:

- RfC #76440: [Csm] duplicated requirement IDs:

  Problem description:

  Following requirement IDs are duplicated @ AUTOSAR CP R4.3.0 SWS Csm.
  [SWS_Csm_00037]: assigned to two similar requirements (clean up required)
  [SWS_Csm_00828]: assigned to two different requirements
  [SWS_Csm_00877]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_01083]: second one seems result of failed "copy & paste" of first one
  [SWS_Csm_00930]: assigned to two different requirements
  [SWS_Csm_00932]: assigned to two different requirements
  [SWS_Csm_00934]: assigned to two different requirements
  –Last change on issue 76440 comment 19–

  Agreed solution:

  SWS_Csm_00037 -> new ID for second
  SWS_Csm_00828 -> new ID for first
  SWS_Csm_00877 -> correction already available (refer to .../Z-

GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_01083 -> correction already available (refer to .../Z-GEN_SWSArtifacts/Service_Interfaces/HTML/Csm.html), just an update of affected artifact needed
SWS_Csm_00930 -> new ID for first
SWS_Csm_00932 -> new ID for first
SWS_Csm_00934 -> new ID for first
–Last change on issue 76440 comment 15–

BW-C-Level:

Application	Specification	Bus
1	1	1

1.105 Specification Item SWS_Csm_91008

Trace References:

none

Content:

While the CSM is not initialized and any function of the CSM API is called, except of CSM_Init(), the operation shall not be performed and CSM_E_UNINIT shall be reported to the DET when CsmDevErrorDetect is true.

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

1.106 Specification Item SWS_Csm_91009

Trace References:

none

Content:

If a pointer to null is passed to an API function, the operation shall not be performed and CSM_E_PARAM_POINTER shall be reported to the DET when CsmDevErrorDetect is true.

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

1.107 Specification Item SWS_Csm_91010

Trace References:

none

Content:

If a CSM API calls a functionality that is not initialized (the Crypto Interface), the operation shall not be performed and CSM_E_SERVICE_NOT_STARTED shall be reported to the DET when CsmDevErrorDetect is true.

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

1.108 Specification Item SWS_Csm_91011

Trace References:

none

Content:

If a CSM API with a key handle in its interface is called and the key handle (called keyID) is out of range, the operation shall not be performed and CSM_E_PARAM_HANDLE shall be reported to the DET when CsmDevErrorDetect is true.

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

1.109 Specification Item SWS_Csm_91012

Trace References:

none

Content:

If a CSM API is called with a buffer too small to perform the desired operation, the operation shall not be performed and CSM_E_SMALL_BUFFER shall be reported to the DET when CsmDevErrorDetect is true.

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