Document Title	SWS_V2XManagement: 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_V2XManagement

1.1 Specification Item SWS_V2xM_00092

Trace References:

none

Content:

API function	Description
Csm_CertificateParse	This function shall dispatch the certificate parse function to the CRYIF.
Csm_CertificateVerify	Verifies the certificate stored in the key referenced by verifyKey Id with the certificate stored in the key referenced by keyId. Note: Only certificates stored in the same Crypto Driver can be verified against each other. If the key element CRYPTO_KE_CERTIFICATE_CURRENT_TIME is used for the verification of the validity period of the certificate indentified by verifyKeyId, it shall have the same format as the timestamp in the certificate.
Csm_Hash	Uses the given data to perform the hash calculation and stores the hash.
Csm_KeyElementGet	Retrieves the key element bytes from a specific key element of the key identified by the keyId and stores the key element in the memory location pointed by the key pointer.
Csm_KeyElementSet	Sets the given key element bytes to the key identified by keyId.
Csm_RandomGenerate	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.
Csm_SignatureGenerate	Uses the given data to perform the signature calculation and stores the signature in the memory location pointed by the result pointer.
Csm_SignatureVerify	Verifies the given MAC by comparing if the signature is generated with the given data.
EthIf_GetChanRxParams	Read values related to the receive direction of the transceiver. For example, this could be a Channel Busy Ratio (CBR) or the average Channel Idle Time (CIT).
EthIf_SetChanRxParams	Set values related to the receive direction of a transceiver's wireless channel. For example, this could be a channel parameter like the frequency.
EthIf_SetChanTxParams	Set values related to the transmit direction of a transceiver's wireless channel. For example, this could be the bitrate of a channel.
EthIf_SetPhysAddr	Sets the physical source address used by the indexed controller.
EthIf_SetRadioParams	Set values related to a transceiver's wireless radio. For example, this could be the selection of the radio settings (channel, ...).
NvM_GetErrorStatus	Service to read the block dependent error/status information.

API function	Description
NvM_ReadBlock	Service to copy the data of the NV block to its corresponding RAM block.
NvM_WriteBlock	Service to copy the data of the RAM block to its corresponding NV block.
V2xFac_V2xM_AbortPseudonymChange	This function is called by the V2xM when not all modules are OK with the pseudonym change and the change is to be rolled back.
V2xFac_V2xM_CommitPseudonymChange	This function is called by the V2xM when all modules are OK with the pseudonym change and the change is to be committed.
V2xFac_V2xM_PreparePseudonymChange	By this API primitive the V2xFac module gets an indication that the Pseudonym and hereby the StationId has changed.
V2xFac_V2xM_SetCaBsOperation	By this API primitive the V2xFac module gets an indication of the current operation state of the CA Basic Service.
V2xFac_V2xM_SetTGenCamDcc	By this API primitive the V2xFac module gets an indication of the current TGenCamDcc value.
V2xGn_V2xM_AbortPseudonymChange	This function is called by the V2xM when not all modules are OK with the pseudonym change and the change is to be rolled back.
V2xGn_V2xM_CommitPseudonymChange	This function is called by the V2xM when all modules are OK with the pseudonym change and the change is to be committed.
V2xGn_V2xM_DecapConfirmation	This function is called by the V2xM when a decapsulation has been finished.
V2xGn_V2xM_EncapConfirmation	This function is called by the V2xM when an encapsulation has been finished.
V2xGn_V2xM_PreparePseudonymChange	This function is called by the V2xM when a Pseudonym Change occurs to prepare the change in every module using it.

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