

|                                   |   |
|-----------------------------------|---|
| <b>Document Title</b>             | Specification of Crypto Service Manager |
| <b>Document Owner</b>             | AUTOSAR                                 |
| <b>Document Responsibility</b>    | AUTOSAR                                 |
| <b>Document Identification No</b> | 402                                     |
| <b>Document Status</b>            | published                               |
| <b>Part of AUTOSAR Standard</b>   | Classic Platform                        |
| <b>Part of Standard Release</b>   | R19-11                                  |

| <b>Document Change History</b> |                |                            |   |
|--------------------------------|----------------|----------------------------|---|
| <b>Date</b>                    | <b>Release</b> | <b>Changed by</b>          | <b>Change Description</b>   |
| 2019-11-28                     | R19-11         | AUTOSAR Release Management | <ul style="list-style-type: none"> <li>• Bringing return values of all services and interfaces to one line</li> <li>• added functionality and description of elliptic curves</li> <li>• Callback notification modified</li> <li>• Editorial changes</li> <li>• Changed Document Status from Final to published</li> </ul> |
| 2018-10-31                     | 4.4.0          | AUTOSAR Release Management | <ul style="list-style-type: none"> <li>• Client-Server-Interfaces Csm&lt;Service&gt;_{Config}</li> <li>• corrected CS interfaces</li> <li>• removal of references to CryptoAbstractionLibrary</li> </ul>  |
| 2017-12-08                     | 4.3.1          | AUTOSAR Release Management | <ul style="list-style-type: none"> <li>• Added definition for asymmetric key formats</li> <li>• Error fixing and consistency improvements</li> <li>• Editorial changes</li> </ul>   |
| 2016-11-30                     | 4.3.0          | AUTOSAR Release Management | <ul style="list-style-type: none"> <li>• Introduced crypto job concept</li> <li>• Introduced key management concept</li> <li>• Removed Cry_XXX functions from the Csm and introduced two new layers in the crypto stack: Crypto Interface (CryIf) and Crypto Driver (Crypto)</li> </ul>                                   |

| <b>Document Change History</b> |                |                            |  |
|--------------------------------|----------------|----------------------------|--|
| <b>Date</b>                    | <b>Release</b> | <b>Changed by</b>          | <b>Change Description</b>  |
| 2015-07-31                     | 4.2.2          | AUTOSAR Release Management | <ul style="list-style-type: none"> <li>• Changed return type from Csm_ReturnType to Std_Types in all API functions</li> <li>• Added detailed description of RTE interfaces</li> <li>• Debugging support marked as obsolete</li> <li>• Error fixing and consistency improvements</li> </ul>   |
| 2014-10-31                     | 4.2.1          | AUTOSAR Release Management | <ul style="list-style-type: none"> <li>• Obsolete configuration elements removed</li> <li>• Error fixing and consistency improvements</li> <li>• Editorial changes</li> </ul>  |
| 2014-03-31                     | 4.1.3          | AUTOSAR Release Management | <ul style="list-style-type: none"> <li>• Error fixing and consistency improvements</li> <li>• Editorial changes</li> </ul>   |
| 2013-10-31                     | 4.1.2          | AUTOSAR Release Management | <ul style="list-style-type: none"> <li>• Error fixing and consistency improvements</li> <li>• Editorial changes</li> <li>• Removed chapter(s) on change documentation</li> </ul>   |
| 2013-03-15                     | 4.1.1          | AUTOSAR Administration     | <ul style="list-style-type: none"> <li>• Services for compression/decompression added</li> <li>• Services for key update added (Concept 'CSM extension')</li> <li>• Services for symmetric key generation added (Concept 'CSM extension')</li> <li>• Service state machine changed to cope with terminated users by releasing of locked resources</li> <li>• Production errors restructured</li> </ul> |
| 2011-12-22                     | 4.0.3          | AUTOSAR Administration     | <ul style="list-style-type: none"> <li>• Fixed issues with AUTOSAR Port Interfaces</li> </ul>  |

| <b>Document Change History</b> |                |                        |   |
|--------------------------------|----------------|------------------------|---|
| <b>Date</b>                    | <b>Release</b> | <b>Changed by</b>      | <b>Change Description</b>   |
| 2010-09-30                     | 3.1.5          | AUTOSAR Administration | <ul style="list-style-type: none"><li>• Complete Configuration parameters</li><li>• Complete API specifications</li><li>• Add support for secure key storage</li><li>• Integration of support for key transport services</li><li>• Introduction of new DET error (checking of the null pointer in getversion info).</li></ul> |
| 2010-02-02                     | 3.1.4          | AUTOSAR Administration | <ul style="list-style-type: none"><li>• Initial release</li></ul>   |

## Disclaimer

This work (specification and/or software implementation) and the material contained in it, as released by AUTOSAR, is for the purpose of information only. AUTOSAR and the companies that have contributed to it shall not be liable for any use of the work. The material contained in this work is protected by copyright and other types of intellectual property rights. The commercial exploitation of the material contained in this work requires a license to such intellectual property rights.

This work may be utilized or reproduced without any modification, in any form or by any means, for informational purposes only. For any other purpose, no part of the work may be utilized or reproduced, in any form or by any means, without permission in writing from the publisher.

The work has been developed for automotive applications only. It has neither been developed, nor tested for non-automotive applications.

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

## Table of Contents

|        |   |    |
|--------|---|----|
| 1      | Introduction and Functional Overview .....    | 8  |
| 2      | Acronyms and Abbreviations.....               | 9  |
| 2.1    | Glossary of Terms .....                       | 9  |
| 3      | Related documentation .....                   | 11 |
| 3.1    | Input Documents .....                         | 11 |
| 3.2    | Related standards and norms .....             | 12 |
| 3.3    | Related specification .....                   | 12 |
| 4      | Constraints and Assumptions.....              | 13 |
| 4.1    | Limitations .....                             | 13 |
| 4.2    | Applicability to Car Domains.....             | 13 |
| 4.3    | Security Implications.....                    | 13 |
| 5      | Dependencies to other Modules.....            | 14 |
| 5.1    | File Structure .....                          | 14 |
| 5.1.1  | Code File Structure .....                     | 14 |
| 6      | Requirements Traceability.....                | 15 |
| 7      | Functional specification .....                | 18 |
| 7.1    | Basic Architecture Guidelines.....            | 18 |
| 7.2    | General Behavior.....                         | 18 |
| 7.2.1  | Normal Operation.....                         | 19 |
| 7.2.2  | Design Notes.....                             | 22 |
| 7.3    | Error Classification .....                    | 31 |
| 7.3.1  | Development Errors .....                      | 31 |
| 7.3.2  | Runtime Errors .....                          | 31 |
| 7.3.3  | Transient Faults .....                        | 31 |
| 7.3.4  | Production Errors .....                       | 31 |
| 7.3.5  | Extended Production Errors .....              | 32 |
| 7.4    | Error detection .....                         | 32 |
| 8      | API Specification .....                       | 33 |
| 8.1    | Imported types.....                           | 33 |
| 8.2    | Type Definitions.....                         | 33 |
| 8.2.1  | Extension to Std_ReturnType .....             | 33 |
| 8.2.2  | Csm_ConfigType .....                          | 33 |
| 8.2.3  | Crypto_AlgorithmFamilyType .....              | 34 |
| 8.2.4  | Crypto_AlgorithmModeType.....                 | 36 |
| 8.2.5  | Crypto_InputOutputRedirectionConfigType ..... | 37 |
| 8.2.6  | Crypto_JobType.....                           | 38 |
| 8.2.7  | Crypto_JobStateType .....                     | 39 |
| 8.2.8  | Crypto_JobPrimitiveInputOutputType .....      | 39 |
| 8.2.9  | Crypto_JobInfoType.....                       | 41 |
| 8.2.10 | Crypto_JobPrimitiveInfoType .....             | 41 |
| 8.2.11 | Crypto_ServiceInfoType.....                   | 42 |
| 8.2.12 | Crypto_JobRedirectionInfoType.....            | 43 |
| 8.2.13 | Crypto_AlgorithmInfoType.....                 | 44 |

|         |  |     |
|---------|--|-----|
| 8.2.14  | Crypto_ProcessingType .....  | 45  |
| 8.2.15  | Crypto_PrimitiveInfoType .....                                       | 45  |
| 8.2.16  | Csm_ConfigIdType .....   | 46  |
| 8.3     | Function Definitions .....   | 46  |
| 8.3.1   | General Interface .....  | 47  |
| 8.3.2   | Hash Interface .....   | 48  |
| 8.3.3   | MAC interface .....  | 49  |
| 8.3.4   | Cipher Interface.....  | 51  |
| 8.3.5   | Authenticated Encryption with Associated Data (AEAD) Interface ..... | 53  |
| 8.3.6   | Signature Interface .....  | 56  |
| 8.3.7   | Random Interface.....  | 58  |
| 8.3.8   | Key Management Interface .....                                       | 59  |
| 8.3.9   | Cryptographic Primitives and Schemes .....                           | 72  |
| 8.3.10  | Job Cancellation Interface.....                                      | 78  |
| 8.3.11  | Callback Notifications .....   | 79  |
| 8.3.12  | Scheduled functions.....   | 80  |
| 8.4     | Expected Interfaces.....   | 80  |
| 8.4.1   | Interfaces to Standard Software Modules .....                        | 80  |
| 8.4.2   | Mandatory Interfaces .....   | 80  |
| 8.4.3   | Optional Interfaces .....  | 81  |
| 8.4.4   | Configurable interfaces .....  | 82  |
| 8.5     | Service Interface.....   | 83  |
| 8.5.1   | Client-Server-Interfaces .....                                       | 83  |
| 8.5.2   | Client-Server-Interfaces (DATA_REFERENCES) .....                     | 106 |
| 8.5.3   | Client-Server-Interfaces (Key Management) .....                      | 124 |
| 8.5.4   | Implementation Data Types .....                                      | 132 |
| 8.5.5   | Ports.....   | 143 |
| 9       | Sequence Diagrams.....   | 146 |
| 9.1     | Asynchronous Calls.....  | 146 |
| 9.2     | Synchronous Calls.....   | 147 |
| 10      | Configuration.....   | 148 |
| 10.1    | How to Read this Chapter .....                                       | 148 |
| 10.2    | Containers and Configuration Parameters .....                        | 148 |
| 10.2.1  | Csm.....   | 149 |
| 10.2.2  | CsmGeneral.....  | 150 |
| 10.2.3  | CsmJobs .....  | 152 |
| 10.2.4  | CsmJob.....  | 153 |
| 10.2.5  | CsmKeys.....   | 156 |
| 10.2.6  | CsmKey .....   | 157 |
| 10.2.7  | CsmQueues .....  | 158 |
| 10.2.8  | CsmQueue .....   | 158 |
| 10.2.9  | CsmInOutRedirections .....   | 161 |
| 10.2.10 | CsmInOutRedirection.....   | 161 |
| 10.2.11 | CsmPrimitives .....  | 164 |
| 10.2.12 | CsmHash .....  | 166 |
| 10.2.13 | CsmHashConfig.....   | 167 |
| 10.2.14 | CsmMacGenerate .....   | 171 |
| 10.2.15 | CsmMacGenerateConfig.....  | 172 |
| 10.2.16 | CsmMacVerify.....  | 176 |

|         |   |     |
|---------|---|-----|
| 10.2.17 | CsmMacVerifyConfig .....                | 177 |
| 10.2.18 | CsmEncrypt.....                         | 181 |
| 10.2.19 | CsmEncryptConfig .....                  | 182 |
| 10.2.20 | CsmDecrypt .....                        | 187 |
| 10.2.21 | CsmDecryptConfig .....                  | 187 |
| 10.2.22 | CsmAEADEncrypt.....                     | 192 |
| 10.2.23 | CsmAEADEncryptConfig .....              | 192 |
| 10.2.24 | CsmAEADDecrypt.....                     | 197 |
| 10.2.25 | CsmAEADDecryptConfig .....              | 197 |
| 10.2.26 | CsmSignatureGenerate .....              | 203 |
| 10.2.27 | CsmSignatureGenerateConfig .....        | 203 |
| 10.2.28 | CsmSignatureVerify .....                | 209 |
| 10.2.29 | CsmSignatureVerifyConfig.....           | 209 |
| 10.2.30 | CsmRandomGenerate .....                 | 215 |
| 10.2.31 | CsmRandomGenerateConfig.....            | 215 |
| 10.2.32 | CsmJobKeySetValid .....                 | 218 |
| 10.2.33 | CsmJobKeySetValidConfig .....           | 218 |
| 10.2.34 | CsmJobRandomSeed .....                  | 221 |
| 10.2.35 | CsmJobRandomSeedConfig.....             | 221 |
| 10.2.36 | CsmJobKeyDerive .....                   | 224 |
| 10.2.37 | CsmJobKeyDeriveConfig .....             | 225 |
| 10.2.38 | CsmJobKeyGenerate.....                  | 227 |
| 10.2.39 | CsmJobKeyGenerateConfig.....            | 228 |
| 10.2.40 | CsmJobKeyExchangeCalcPubVal .....       | 230 |
| 10.2.41 | CsmJobKeyExchangeCalcPubValConfig.....  | 231 |
| 10.2.42 | CsmJobKeyExchangeCalcSecret .....       | 234 |
| 10.2.43 | CsmJobKeyExchangeCalcSecretConfig ..... | 235 |
| 10.2.44 | CsmCallbacks .....                      | 237 |
| 10.2.45 | CsmCallback.....                        | 237 |
| 10.3    | Published Information.....              | 238 |

## 1 Introduction and Functional Overview

This specification specifies the functionality, API and the configuration of the software module Crypto Service Manager (CSM) to satisfy the top-level requirements represented in the CSM Requirements Specification (SRS) [CSM\_SRS].

The CSM shall provide synchronous or asynchronous services to enable a unique access to basic cryptographic functionalities for all software modules. The CSM shall provide an abstraction layer, which offers a standardized interface to higher software layers to access these functionalities.

The functionality required by a software module can be different to the functionality required by other software modules. For this reason, there shall be the possibility to configure and initialize the services provided by the CSM individually for each software module. This configuration comprises as well the selection of synchronous or asynchronous processing of the CSM services.

The construction of the CSM module follows a generic approach. Wherever a detailed specification of structures and interfaces would limit the scope of the usability of the CSM, interfaces and structures are defined in a generic way. This provides an opportunity for future extensions.



## 2 Acronyms and Abbreviations

Acronyms and abbreviations, which have a local scope and therefore are not contained in the AUTOSAR glossary [13], are listed in this chapter.

| <b>Abbreviation / Acronym:</b> | <b>Description:</b>                           |
|--------------------------------|---|
| AEAD                           | Authenticated Encryption with Associated Data |
| CDD                            | Complex Device Driver                         |
| CSM                            | Crypto Service Manager                        |
| CRYIF                          | Crypto Interface                              |
| CRYPTO                         | Crypto Driver                                 |
| DET                            | Default Error Tracer                          |
| HSM                            | Hardware Security Module                      |
| HW                             | Hardware                                      |
| SHE                            | Security Hardware Extension                   |
| SW                             | Software                                      |

### 2.1 Glossary of Terms

| <b>Terms:</b>        | <b>Description:</b>  |
|----------------------|--|
| Crypto Driver Object | A Crypto Driver implements one or more Crypto Driver Objects. The Crypto Driver Object can offer different crypto primitives in hardware or software. The Crypto Driver Objects of one Crypto Driver are independent of each other. There is only one workspace for each Crypto Driver Object (i.e. only one crypto primitive can be performed at the same time) |
| Key                  | A Key can be referenced by a job in the Csm. In the Crypto Driver, the key refers a specific key type.   |
| Key Type             | A key type consists of refers to key elements. The key types are typically pre-configured by the vendor of the Crypto Driver.  |
| Key Element          | Key elements are used to store data. This data can be e.g. key material or the IV needed for AES encryption. It can also be used to configure the behaviour of the key management functions.   |
| Job                  | A Job is a configured 'CsmJob'. Among others, it refers to a key, a cryptographic primitive and a reference channel.   |
| Channel              | A channel is the path from a Crypto Service Manager queue via the Crypto Interface to a specific Crypto Driver Object.   |
| Primitive            | A primitive is an instance of a configured cryptographic algorithm realized in a Crypto Driver Object. Among others it refers to a functionality provided by the CSM to the application, the concrete underlining 'algorithmfamily' (e.g. AES, MD5, RSA, etc.), and a 'algorithmmode' (e.g. ECB, CBC, etc).  |
| Operation            | An operation of a crypto primitive declares what part of the crypto  |

|            |   |   |
|------------|---|---|
|            | primitive shall be performed. There are three different operations:   |   |
|            | START   | Operation indicates a new request of a crypto primitive, it shall cancel all previous requests perform necessary initializations and checks if the crypto primitive can be processed. |
|            | UPDATE  | Operation indicates, that the crypto primitive expect input data. An update operation may provide intermediate results.   |
|            | FINISH  | Operation indicates, that after this part all data are fed completely and the crypto primitive can finalize the calculations. A finish operation may provide final results.           |
|            | It is also possible to perform more than one operation at once by concatenating the corresponding bits of the operation_mode argument.  |   |
| Priority   | The priority of a job defines the importance of it. The higher the priority (as well in value), the more immediate the job will be executed. The priority of a cryptographic job is part of the configuration.  |   |
| Processing | Indicates the kind of job processing.   |   |
|            | Asynchronous  | The job is not processed immediately when calling a corresponding function. Usually, the caller is informed via a callback function when the job has been finished.                   |
|            | Synchronous   | The job is processed immediately when calling a corresponding function. When the function returns, a result will be available.  |
| Service    | A service shall be understand as defined in the TR_Glossary document: A service is a type of operation that has a published specification of interface and behavior, involving a contract between the provider of the capability and the potential clients. |   |

## 3 Related documentation

### 3.1 Input Documents

- [1] List of Basic Software Modules  
AUTOSAR\_TR\_BSWModuleList.pdf
  
- [2] Layered Software Architecture  
AUTOSAR\_EXP\_LayeredSoftwareArchitecture.pdf
  
- [3] General Requirements on Basic Software Modules  
AUTOSAR\_SRS\_BSWGeneral.pdf
  
- [4] Specification of RTE Software  
AUTOSAR\_SWS\_RTE.pdf
  
- [5] Specification of BSW Scheduler  
AUTOSAR\_SWS\_Scheduler.pdf
  
- [6] Specification of ECU Configuration  
AUTOSAR\_TPS\_ECUConfiguration.pdf
  
- [7] Specification of Memory Mapping  
AUTOSAR\_SWS\_MemoryMapping.pdf
  
- [8] Specification of Default Error Tracer  
AUTOSAR\_SWS\_DefaultErrorTracer.doc.pdf
  
- [9] Specification of Diagnostic Event Manager  
AUTOSAR\_SWS\_DiagnosticEventManager.pdf
  
- [10] Specification of ECU State Manager  
AUTOSAR\_SWS\_ECUCStateManager.pdf
  
- [11] Specification of C Implementation Rules  
AUTOSAR\_TR\_CImplementationRules.pdf
  
- [12] Specification of Standard Types  
AUTOSAR\_SWS\_StandardTypes.pdf
  
- [13] AUTOSAR Glossary  
AUTOSAR\_TR\_Glossary.pdf
  
- [14] Requirements on the Crypto Stack  
AUTOSAR\_SRS\_CryptoStack.pdf
  
- [15] Specification of the Crypto Interface  
AUTOSAR\_SWS\_CryptoInterface.pdf

[16] Specification of the Crypto Driver  
AUTOSAR\_SWS\_CryptoDriver.pdf

[17] General Specification of Basic Software Modules  
AUTOSAR\_SWS\_BSWGeneral.pdf

### **3.2 Related standards and norms**

[18] IEC 7498-1 The Basic Model, IEC Norm, 1994

[19] IETF RFC5639 Elliptic Curve Cryptography (ECC) Brainpool Standard  
Curves and Curve Generation, 2010

[20] IETF RFC6637 Elliptic Curve Cryptography (ECC) in OpenPGP, 2012

### **3.3 Related specification**

AUTOSAR provides a General Specification on Basic Software modules (SWS BSW General), which is also valid for Crypto Service Manager.

Thus, the specification SWS BSW General shall be considered as additional and required specification for Crypto Service Manager.

## 4 Constraints and Assumptions

### 4.1 Limitations

Some type definitions of CSM start with the Prefix “CRYPTO\_” which will violate SRS\_BSW\_00305. This will be harmonized in release 4.3.1. Nevertheless due to the constraint [constr\_1050] part 1 the ports are still consider to be compatible.

### 4.2 Applicability to Car Domains

n.a.

### 4.3 Security Implications

There is no user management in place, which prevents non-authorized access on any of CSM’s services. This means, that if any access protection is needed such must be implemented by the application and the served (by CSM) cryptographic library modules; access protection is not target of the CSM.

## 5 Dependencies to other Modules

**[SWS\_Csm\_00001]** [The CSM shall be able to access the cryptographic interface (CRYIF), which is implemented according to the cryptographic interface specification. ](SRS\_CryptoStack\_00082)

**[SWS\_Csm\_00506]** [The CSM module shall use the interfaces of the CRYIF with the underlying Crypto Drivers (CRYPTO) to calculate the result of a cryptographic service.

](SRS\_CryptoStack\_00082)

The incorporated cryptographic library modules or hardware extensions of the Crypto Driver provide the cryptographic routines, e.g. SHA-1, RSA, AES, Diffie-Hellman key-exchange, etc.

### 5.1 File Structure

#### 5.1.1 Code File Structure

**[SWS\_Csm\_00002]** [The code file structure shall not be defined within this specification completely. The CSM module shall consist of the following parts:

]()

## 6 Requirements Traceability

| Requirement           | Description  | Satisfied by   |
|-----------------------|--|--|
| SRS_BSW_00101         | The Basic Software Module shall be able to initialize variables and hardware in a separate initialization function | SWS_Csm_00646  |
| SRS_BSW_00358         | The return type of init() functions implemented by AUTOSAR Basic Software Modules shall be void                    | SWS_Csm_00646  |
| SRS_BSW_00359         | All AUTOSAR Basic Software Modules callback functions shall avoid return types other than void if possible         | SWS_Csm_00970, SWS_Csm_00971                               |
| SRS_BSW_00360         | AUTOSAR Basic Software Modules callback functions are allowed to have parameters                                   | SWS_Csm_00970, SWS_Csm_00971                               |
| SRS_BSW_00373         | The main processing function of each AUTOSAR Basic Software Module shall be named according the defined convention | SWS_Csm_00479  |
| SRS_BSW_00407         | Each BSW module shall provide a function to read out the version information of a dedicated module implementation  | SWS_Csm_00705  |
| SRS_BSW_00414         | Init functions shall have a pointer to a configuration structure as single parameter                               | SWS_Csm_00646  |
| SRS_BSW_00432         | Modules should have separate main processing functions for read/receive and write/transmit data path               | SWS_Csm_00479  |
| SRS_CryptoStack_00008 | The Crypto Stack shall allow static configuration of keys used for cryptographic jobs                              | SWS_Csm_00951, SWS_Csm_00953, SWS_Csm_01012, SWS_Csm_01092 |
| SRS_CryptoStack_00009 | The Crypto Stack shall support reentrancy for all crypto services  | SWS_Csm_00022  |
| SRS_CryptoStack_00010 | The Crypto Stack shall conceal symmetric keys from the users of crypto services                                    | SWS_Csm_00959  |
| SRS_CryptoStack_00011 | The Crypto Stack shall conceal asymmetric private keys from the users of Crypto services                           | SWS_Csm_00959  |
| SRS_CryptoStack_00019 | The Crypto Stack shall identify random number generation as  | SWS_Csm_01543  |

|                       |   |   |
|-----------------------|---|---|
|                       | a cryptographic primitive which can be requested to a driver  |   |
| SRS_CryptoStack_00020 | The Crypto Stack shall identify symmetric encryption/decryption as a cryptographic primitive which can be requested to a driver                     | SWS_Csm_00984, SWS_Csm_00989  |
| SRS_CryptoStack_00021 | The Crypto Stack shall identify asymmetric encryption/decryption as a cryptographic primitive which can be requested to a driver                    | SWS_Csm_00984, SWS_Csm_00989  |
| SRS_CryptoStack_00022 | The Crypto Stack shall identify MAC generation/verification as a cryptographic primitive which can be requested to a driver                         | SWS_Csm_00982   |
| SRS_CryptoStack_00023 | The Crypto Stack shall identify asymmetric signature generation/verification as a cryptographic primitive which can be requested to a driver        | SWS_Csm_00992, SWS_Csm_00996  |
| SRS_CryptoStack_00024 | The Crypto Stack shall identify hash calculation as a cryptographic primitive which can be requested to a driver                                    | SWS_Csm_00980   |
| SRS_CryptoStack_00026 | The Crypto Stack shall provide an interface for the generation of asymmetric keys   | SWS_Csm_00955   |
| SRS_CryptoStack_00027 | The Crypto Stack shall provide an interface for the generation of symmetric keys  | SWS_Csm_00955   |
| SRS_CryptoStack_00082 | The CSM module specification shall specify the interface and behavior of the callback function, if the asynchronous job processing mode is selected | SWS_Csm_00001, SWS_Csm_00032, SWS_Csm_00506   |
| SRS_CryptoStack_00084 | The CSM module shall use the streaming approach for some selected services  | SWS_Csm_01039   |
| SRS_CryptoStack_00086 | The CSM module shall distinguish between error types  | SWS_Csm_01089, SWS_Csm_91004  |
| SRS_CryptoStack_00087 | The CSM module shall report detected development errors to the Default Error Tracer   | SWS_Csm_01088, SWS_Csm_01091  |
| SRS_CryptoStack_00090 | The CSM shall provide an interface to be accessible via the RTE   | SWS_Csm_00802, SWS_Csm_00803, SWS_Csm_00902, SWS_Csm_00903, SWS_Csm_00912, SWS_Csm_00922, SWS_Csm_00923, SWS_Csm_00927, SWS_Csm_00928, SWS_Csm_00930, |



|                        |   |   |
|------------------------|---|---|
|                        |   | SWS_Csm_00934, SWS_Csm_00935, SWS_Csm_00936, SWS_Csm_00943, SWS_Csm_00946, SWS_Csm_01042, SWS_Csm_01074, SWS_Csm_01075, SWS_Csm_01077, SWS_Csm_01078, SWS_Csm_01079, SWS_Csm_01906, SWS_Csm_01910, SWS_Csm_01915, SWS_Csm_01920, SWS_Csm_01921, SWS_Csm_01922, SWS_Csm_01923, SWS_Csm_01924, SWS_Csm_01925, SWS_Csm_01926, SWS_Csm_01927, SWS_Csm_01928, SWS_Csm_09000, SWS_Csm_91023, SWS_Csm_91051, SWS_Csm_91052, SWS_Csm_91053, SWS_Csm_91054, SWS_Csm_91055, SWS_Csm_91056, SWS_Csm_91057, SWS_Csm_91058, SWS_Csm_91059, SWS_Csm_91060, SWS_Csm_91061, SWS_Csm_91062 |
| SRS_CryptoStack_00091  | The CSM shall provide one Provide--Port for each configuration                      | SWS_Csm_00934, SWS_Csm_01042, SWS_Csm_91023, SWS_Csm_91062  |
| SRS_CryptoStack_00095  | The Crypto Driver module shall strictly separate error and status information       | SWS_Csm_91001, SWS_Csm_91043, SWS_Csm_91044   |
| SRS_CryptoStack_00100  | Synchronous Job Processing  | SWS_Csm_01049   |
| SRS_CryptoStack_00101  | Asynchronous Job Processing   | SWS_Csm_01049   |
| SRS_CryptoStack_00102  | The priority of a user and its crypto jobs shall be defined by static configuration | SWS_Csm_01010   |
| SRS_CryptoStack_00103  | The Crypto Stack shall provide an interface for the derivation of symmetric keys    | SWS_Csm_00956   |
| SRS_CryptoStack_00906  | -   | SWS_Csm_00947   |
| SRS_CryptoStack_01076  | -   | SWS_Csm_01083   |
| SRS_CrypttoStack_00028 | -   | SWS_Csm_00966, SWS_Csm_00967  |
| SRS_CrypttoStack_00029 | -   | SWS_Csm_00959   |
| SRS_Csm_00066          | -   | SWS_Csm_00691, SWS_Csm_01905  |
| SWS_BSW_00050          | Check parameters passed to Initialization functions                                 | SWS_Csm_00186   |
| SWS_BSW_00216          | -   | SWS_Csm_01085   |

## 7 Functional specification

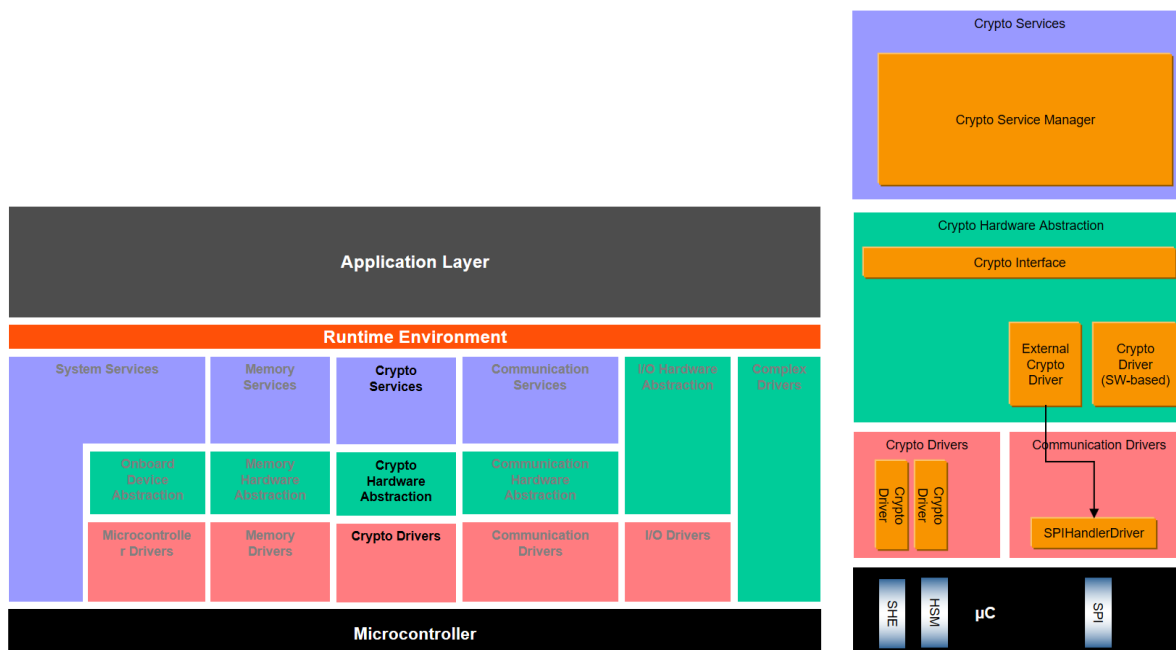


Figure 7-1 AUTOSAR Layered View with CSM

### 7.1 Basic Architecture Guidelines

The starting point for the description of the design of the CSM module is the AUTOSAR Layered Software Architecture (see Figure 7-1). The description of the CSM module architecture on the basis of the AUTOSAR layered software architecture shall help to understand the specification of interfaces and functionalities of the CSM module in the following sections.

The architecture of AUTOSAR consists of several layers which can be seen in Figure 7-1. The Service Layer is the highest layer of the Basic Software. Its task is to provide basic services for application and basic software modules, i.e. it offers the most relevant functionalities for application software and basic software modules.

CSM is a service that provides cryptography functionality, based on a crypto driver which relies on a software library or on a hardware module. Also, mixed setups with multiple crypto drivers are possible. The CSM accesses the different CryptoDrivers over the CRYIF.

### 7.2 General Behavior

**[SWS\_Csm\_00941]** [A job is an instance of a configured cryptographic primitive.  
 ]()

**[SWS\_Csm\_00016]** [ For each job just one instance shall be processed by CSM at a time.

]()

**[SWS\_Csm\_00022]** [The CSM module shall allow parallel processing of different jobs.

](SRS\_CryptoStack\_00009)

**[SWS\_Csm\_00017]** [If a service of the CSM module is requested and the corresponding job is in "ACTIVE" state, the job request shall call

`CryIf_ProcessJob()` and pass on the return value.

]()

**[SWS\_Csm\_00018]** [If a service of the CSM module is requested, and the CSM job needs to be queued and the queue is full, the job request shall be rejected with the return value `CRYPTO_E_BUSY`.

]()

**[SWS\_Csm\_00019]** [If an asynchronous interface is configured, the CSM module shall provide a main function `Csm_MainFunction()` which is called cyclically to control processing of the jobs via a state machine.

]()

### 7.2.1 Normal Operation

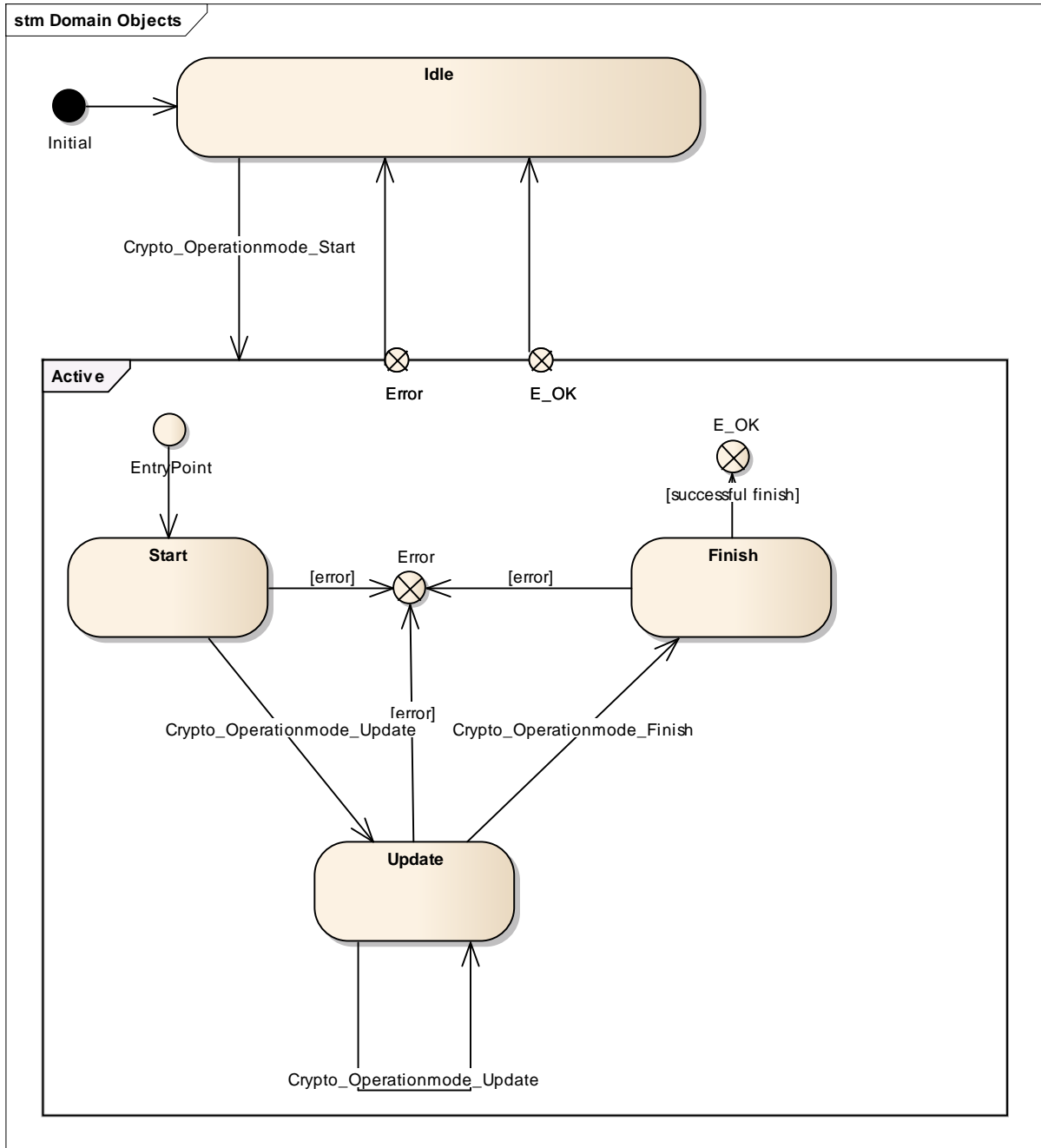
**[SWS\_Csm\_01039]** [To unite a single call function and the streaming approach for the crypto services, there is the `mode` parameter, which determines the operation mode. This service operation is a flag field, indicating the operation mode "START", "UPDATE" or "FINISH". It declares explicitly what operation shall be performed. These operation modes can be mixed, and execute multiple operations at once.

The diagram in **SWS\_Csm\_00024** shows the state machine of a job of this design.

](SRS\_CryptoStack\_00084)

Note: The actual transaction of the states is made in the layer, which works with these states, i.e. in the Crypto Driver.

**[SWS\_Csm\_00024]** [



l()

**[SWS\_Csm\_01033]** The CSM crypto services shall support to process multiple operation mode inputs with a single call.

l()

**[SWS\_Csm\_01045]** If the `CRYPTO_OPERATIONMODE_START` and `CRYPTO_OPERATIONMODE_FINISH` bits are set and the `CRYPTO_OPERATIONMODE_UPDATE` is not set, the `Csm_<Service>()` function shall return with `E_NOT_OK`.

l()

Note: The coherent single call approach could improve the performance due to less overhead. Instead of calling the explicit API multiple times, only one call is necessary. This approach is intended to be used with small data input, which demand fast processing.

While operating with the streaming approach (“Start”, “Update”, “Finish”) the dedicated Crypto Driver Object is waiting for further input (“Update”) until the “Finish” state has been reached. No other job could be processed on this Crypto Driver instance meanwhile.

### 7.2.1.1 Configuration

**[SWS\_Csm\_91005]** [Each crypto primitive configuration shall be realized as a constant structure of type `Crypto_PrimitiveInfoType`.

]()

**[SWS\_Csm\_91006]** [Each job primitive configuration shall be realized as a constant structure of type `Crypto_JobPrimitiveInfoType`.

]()

**[SWS\_Csm\_00028]** [It shall be possible to create several configurations for each cryptographic primitive.

]()

One configuration per job per primitive is possible.

**[SWS\_Csm\_00029]** [When creating a primitive configuration, it shall be possible to configure all available and allowed schemes from the underlying Crypto Driver Object.

]()

**[SWS\_Csm\_00032]** [If the asynchronous interface is chosen, each job primitive configuration shall contain a callback function.

](SRS\_CryptoStack\_00082)

### 7.2.1.2 Synchronous Job Processing

**[SWS\_Csm\_00035]** [When the synchronous interface is used, the interface functions shall immediately compute the result with the help of the underlying Crypto Stack modules.

]()

**[SWS\_Csm\_00037]** [ If a synchronous job is issued and the priority is greater than the highest priority available in the queue, the CSM shall disable processing new jobs from the queue until the next call of the main function has finished that follows after completion of the currently processed job.

]()

Note:

Channels may hold jobs of both asynchronous and synchronous processing type. If

so, a synchronous job might not be accepted for processing although its job's priority is higher than those of all asynchronous jobs.

Note:

As the underlying Crypto Driver can have its own queue, it can not always be ensured that the highest priority job provided by the application is processed next.

**[SWS\_Csm\_91007]** [ If a synchronous job is issued and the priority is less than the highest priority available in the queue, the CSM shall return `CRYPTO_E_BUSY`.

]()

Note:

By pausing calls to the CSM main function with e.g. critical sections during calling the synchronous jobs, it can be ensured, that synchronous jobs can be processed in a row without having to wait for asynchronous jobs in between if they have a high enough priority. Also consider disabling queueing in the Crypto Driver Object to ensure fast processing of synchronous jobs.

If the loading of asynchronous jobs from the queue shall not be paused by synchronous jobs, the priorities of the synchronous jobs have to be smaller than the asynchronous jobs.

### 7.2.1.3 Asynchronous Job Processing

**[SWS\_Csm\_00036]** [If the asynchronous interface is used, the interface functions shall only hand over the necessary information to the underlying Crypto Stack modules.

]()

**[SWS\_Csm\_00039]** [The users of the CSM shall be notified when a requested cryptographic service has been processed by calling the callback function from the job primitive configuration.

]()

## 7.2.2 Design Notes

The CSM provides two services: (1) the crypto services itself and (2) key management.

### 7.2.2.1 CSM module startup

The `Csm_Init()` request shall not be responsible to trigger the initialization of the underlying CRYIF. It is assumed, that the underlying CRYIF will be initialized by any appropriate entity (e.g. BswM).

Software components, which are using the CSM module, shall be responsible for checking global error and status information resulting from the CSM module startup.

### 7.2.2.2 Crypto Services

#### 7.2.2.2.1 Usage of the CSM crypto services

**[SWS\_Csm\_00734]** [CSM crypto services shall provide a `Csm_<Service>()` API.  
]()

**[SWS\_Csm\_00924]** [The application shall be able to call `Csm_<Service>()` with the operation mode `CRYPTO_OPERATIONMODE_START` to initialize cryptographic computations.  
]()

**[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.  
]()

**[SWS\_Csm\_01046]** [The application shall be able to call `Csm_<Service>()` with the operation mode `CRYPTO_OPERATIONMODE_FINISH` to finalize cryptographic computations.  
]()

**[SWS\_Csm\_00937]** [The deprecated `Csm_<Service>Start()` functions shall be mapped to the `Csm_KeyElementSet()` function and the `Csm_<Service>()` functions with the operation mode "start".  
]()

**[SWS\_Csm\_00938]** [The deprecated `Csm_<Service>Update()` functions shall be mapped to the `Csm_<Service>()` functions with the operation mode "update".  
]()

**[SWS\_Csm\_00939]** [The deprecated `Csm_<Service>Finish()` functions shall be mapped to the `Csm_<Service>()` functions with the operation mode "finish".  
]()

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.

**[SWS\_Csm\_01093]** [If the CSM issues either the service `CRYPTO_MACGENERATE`, `CRYPTO_MACVERIFY`, `CRYPTO_ENCRYPT`, `CRYPTO_DECRYPT`,

CRYPTO\_AEADENCRYPT, CRYPTO\_AEADDECRYPT, CRYPTO\_SIGNATUREGENERATE or CRYPTO\_SIGNATUREVERIFY to the Crypto Interface, it need to make sure that the element `jobPrimitiveInfo->cryIfKeyId` in the job structure of `Crypto_JobType` references to the assigned key of this job.

]()

Note: The Crylf is responsible to transform this ID to the corresponding key ID of the respective crypto driver.

**[SWS\_Csm\_01094]** [If one of the primitive services CRYPTO\_KEYSETVALID, CRYPTO\_RANDOMSEED, CRYPTO\_KEYGENERATE, CRYPTO\_KEYDERIVE, CRYPTO\_KEYEXCHANGEALCPUBVAL or CRYPTO\_KEYEXCHANGEALCSECRET are to be executed, the CSM shall fill in the elements of the structure `Csm_JobType->jobPrimitiveInputOutput->cryIfKeyId` and, if applicable, `Csm_JobType->jobPrimitiveInputOutput->targetCryIfKeyId` with the corresponding Crylf key ID.

]()

Note: The Crylf is responsible to transform these IDs to the corresponding key IDs of the respective crypto driver.

#### 7.2.2.2.2 Queuing

The CSM may have several queues, where the jobs are lining up depending on their priority, to process multiple cryptographic requests. The path from a CSM queue via the Crylf to a Crypto Driver Object is called a *channel*. Each queue of the CSM is mapped to one channel to access the crypto primitives of the Crypto Driver Object. The size of the queue is configurable.

To optimize the hardware usage of the Crypto Driver Object, there is optionally a queue in Crypto Driver, too.

A Crypto Driver Object represents an instance of an independent crypto “device” (hardware or software, e.g. AES accelerator). There could be a channel for fast AES and CMAC calculations on an HSM for jobs with high priority, which ends on a native AES calculation service in the Crypto Driver. But it is also possible, that a Crypto Driver Object is a piece of software, e.g. for RSA calculations where users are able to encrypt, decrypt, sign or verify data.



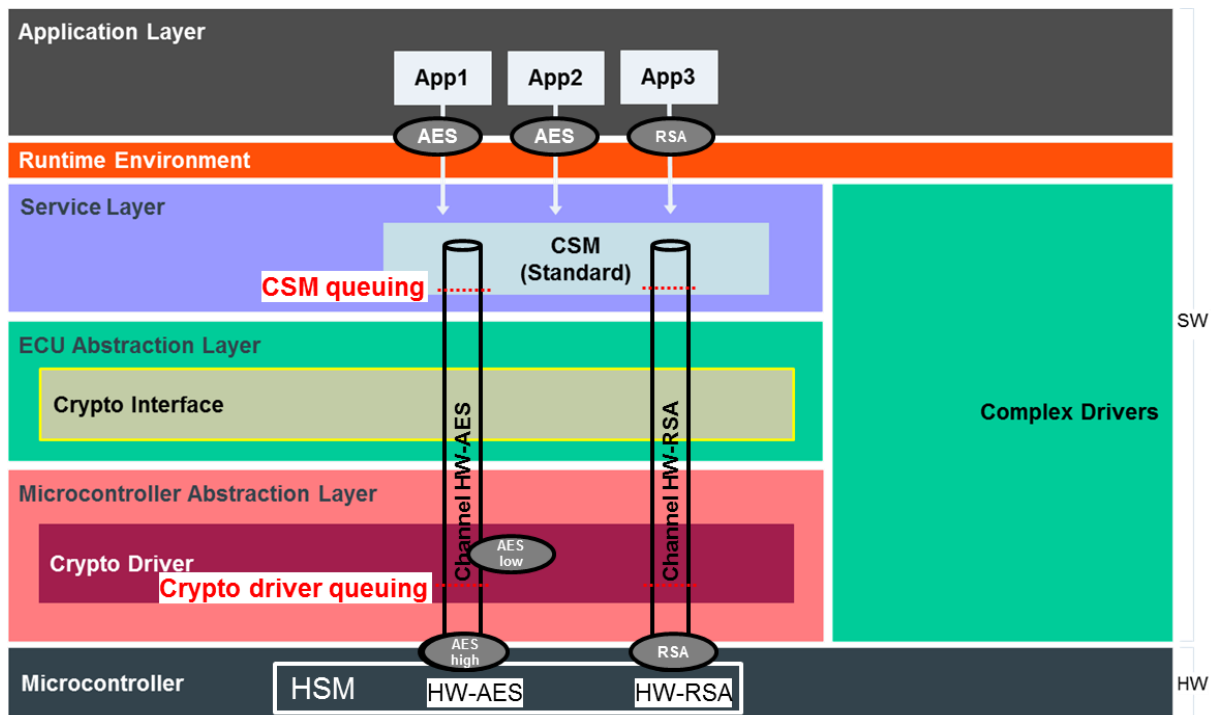


Figure 7-2 AUTOSAR Layered View with channels

Figure 7-2 illustrates an AUTOSAR Layered View with channels. In this example, there is a HSM with two Crypto Driver Objects (HW-AES and HW-RSA), each of them has an own channel. Each channel is connected to a CSM queue and a Crypto Driver Object queue.

In this case, both Crypto Driver Objects are processing a crypto job (AES-high and RSA) each, while the queue of the Crypto Driver Object contains one more job (AES-low). If the HW-AES of the HSM finished the AES-high job, AES-low job will be processed as next one.

Other scenarios with the same setup (without jobs in process or in queues) can be derived as follows:

It will be assumed, that a new job of an application calls RSA.

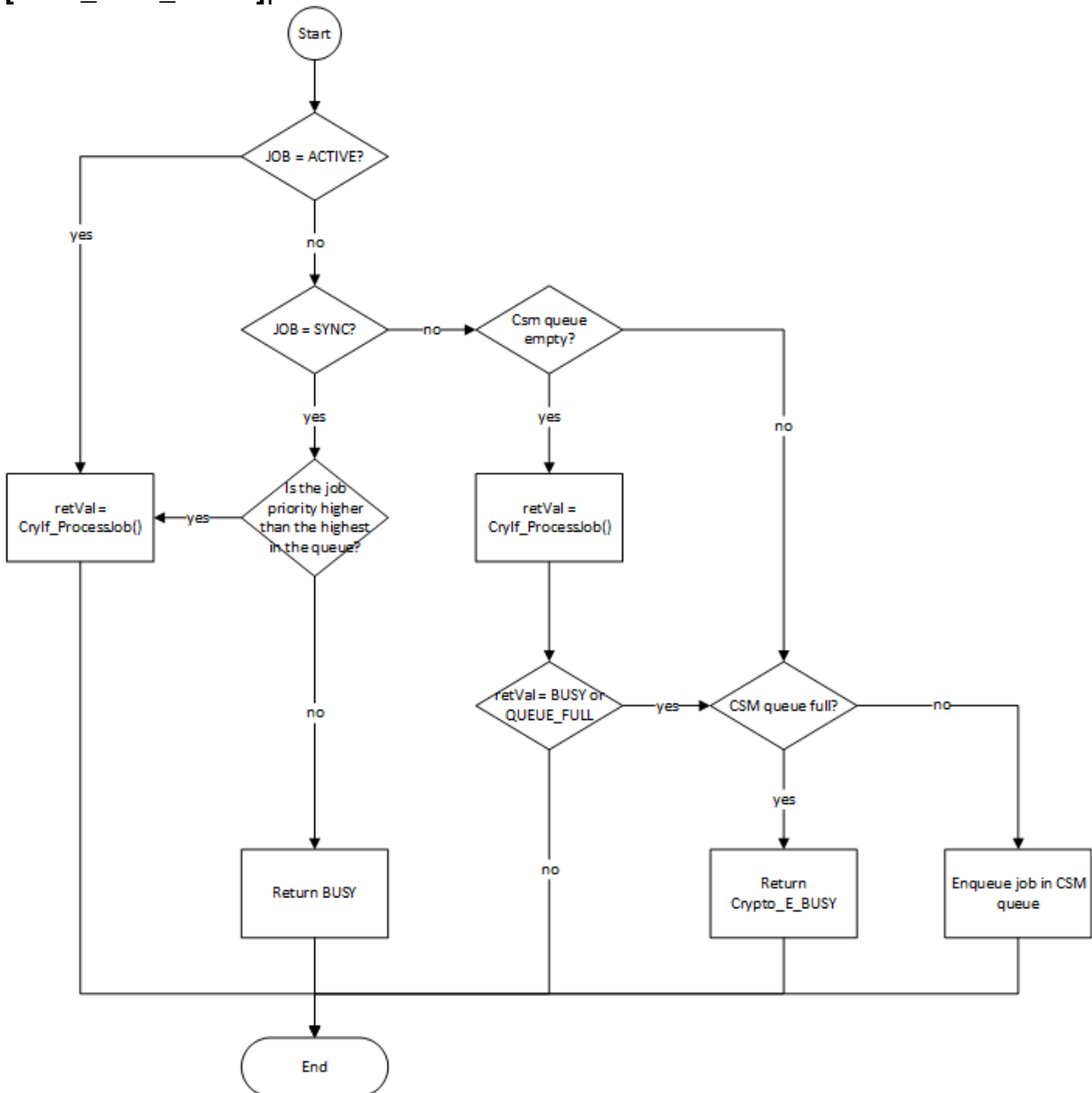
- If the Crypto Driver Object of the RSA is not busy, the job will be processed immediately.
- If the Crypto Driver Object of the RSA is busy, but the queue of the Crypto Driver Object is not full, the job will be listed into that queue in order of its priority. As soon as the Crypto Driver Object is free, the job with the highest priority from the Crypto Driver Object queue will be executed.
- If the Crypto Driver Object of the RSA is busy and the queue of the Crypto Driver Object is full, the job will be stored in the CSM queue in order of its priority.
- If the Crypto Driver Object of the RSA is busy and the queue of the Crypto Driver Object as well as the CSM queue are full, the CSM rejects the request.
- If the Crypto Driver Object of the RSA is active, the job is already started in the Crypto Driver and is waiting for either more data to process or the finish command.

**[SWS\_Csm\_00940]** [It shall be possible to queue CSM jobs in configured CsmQueues in the CSM.  
]()

**[SWS\_Csm\_00944]** [The CsmQueues shall sort the jobs according to the configured job's priority.  
]()  
The higher the job priority value, the higher the job's priority.

**[SWS\_Csm\_00945]** [The Csm\_<Service>() function shall behave as shown in diagram SWS\_Csm\_01041.  
]()

**[SWS\_Csm\_01041]**



]()

Synchronous job processing and queuing might not be useful. So, if synchronous job processing is chosen, the queue sizes should be “0”. However, it is also possible to use channels (including queues) with synchronous and asynchronous jobs.

The queued jobs can be passed to the CRYIF in the `Csm_MainFunction()`.

If the job has the state “active” the CSM shall assume, that the mapped cryptographic driver instance is currently processing this job and the caller wants to continue with the operation (e.g. feeding more data using “update”). The plausibility check has to be performed in the cryptographic driver instance.

### 7.2.2.3 Key Management

**[SWS\_Csm\_00950]** [Services belonging to the key management shall provide the `Csm_<Service>()` function, only.  
]()

**[SWS\_Csm\_00954]** [A key consists of one or more key elements.  
]()

Examples of key elements are the key material itself, an initialization vector, a seed for random number generation, or the proof of the SHE standard.

Keys, i.e. the corresponding key IDs have symbolic names given by the configuration. The Crypto Stack API uses the following key element index definition from the CSM module:

**[SWS\_Csm\_01022]** [

| <i>Crypto Service:</i> | <i>key element:</i> | <i>key element Name:</i>      | <i>key element ID:</i> | <i>Mandatory:</i> |
|------------------------|---------------------|-------------------------------|------------------------|-------------------|
| MAC                    | Key Material        | CRYPTO_KE_MAC_KEY             | 1                      | x                 |
|                        | Proof (SHE)         | CRYPTO_KE_MAC_PROOF           | 2                      |                   |
|                        | Seed                | CRYPTO_KE_KEYGENERATE_SEED    | 16                     |                   |
| Signature              | Key Material        | CRYPTO_KE_SIGNATURE_KEY       | 1                      | x                 |
|                        | ECC curve type      | CRYPTO_KE_SIGNATURE_CURVETYPE | 29                     |                   |
| 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  |   |
|                | 2 <sup>nd</sup> 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_OWNPUKEY     | 10 | x |
|                | Shared Value                 | CYRPTO_KE_KEYEXCHANGE_SHAREDVALUE  | 1  | x |
|                | Algorithm                    | CRYPTO_KE_KEYEXCHANGE_ALGORITHM    | 12 |   |
|                | ECC curve type               | CRYPTO_KE_KEYEXCHANGE_CURVETYPE    | 29 |   |
| 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 |   |
|                | ECC curve type               | CRYPTO_KE_KEYDERIVATION_CURVETYPE  | 29 |   |
| Key Generate   | Key Material                 | CRYPTO_KE_KEYGENERATE_KEY          | 1  | x |
|                | Seed                         | CRYPTO_KE_KEYGENERATE_SEED         | 16 |   |
|                | Algorithm                    | CRYPTO_KE_KEYGENERATE_ALGORITHM    | 17 |   |
|                | ECC curve type               | CRYPTO_KE_KEYGENERATE_CURVETYPE    | 29 |   |

I()

The key elements indices of **SWS\_Csm\_1022** can be extended by the vendor.

**[SWS\_Csm\_00951]** [For 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.

I(SRS\_CryptoStack\_00008)

**[SWS\_Csm\_00953]** [The following key formats are available:

|   |  |
|---|--|
| CRYPTO_KE_FORMAT_BIN_OCTET                  | Key provided as octet value in binary form <sup>1</sup> .            |
| 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.             |

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

$$X = x_{xLen-1} * 256^{xLen-1} + x_{xLen-2} * 256^{xLen-2} + \dots + x_1 * 256 + x_0.$$
 where  $0 \leq x_i < 256$ .

Let the Octet  $X_i$  have the integer value  $x_{xLen-i}$  for  $1 \leq i \leq xLen$ . The octet is then

$$X = X_1 X_2 \dots X_{xLen}$$

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.

](SRS\_CryptoStack\_00008)

**[SWS\_Csm\_00952]** [Vendor specific keyElementIds should start 1000 to avoid interferences with future extended versions of the Crypto Stack.

]()

Note:

The key elements `CRYPTO_KE_[... ]_ALGORITHM` are used to configure the behavior of the key management functions, because they are independent of jobs and therefore can not be configured like a primitive.

**[SWS\_Csm\_01092]** [If a cryptographic primitive uses elliptic curve algorithm but the concrete curve parameter cannot sufficiently specified by its algorithm families and its algorithm mode, an additional key element of type `CRYPTO_KE_XXXXX_CURVETYPE` shall be used to provide the required information. This information is set at runtime through the key element interface. The data of the key element shall be set with its object identifier follows the format defined in [19] and [20].

](SRS\_CryptoStack\_00008)

Example: Definition for an ECC Brainpool 160 P1 key used for signature generation.

```
P2CONST(uint8, AUTOMATIC, MSN_CONST) EccKey =
```

```

{ 0x12, 0x23, 0x34, ... }
; // The required key value.

// According to RFC5639:
// {iso(1) identified-organization(3) teletrust(36)
algorithm(3) signatureAlgorithm(3) ecSign(2)
ecStdCurvesAndGeneration(8) ellipticCurve(1)}

brainpoolP160r1(1)
P2CONST(uint8, AUTOMATIC, MSN_CONST) EccType =
{ 1, 3, 36, 3, 3, 2, 8, 1, 1 }
; //OID definition of ECC Brainpool 160 P1

Csm_KeyElementSet(MyEccKeyId, CRYPTO_KE_SIGNATURE_KEY, EccKey,
sizeof(EccKey) );
Csm_KeyElementSet(MyEccKeyId, CRYPTO_KE_SIGNATURE_CURVETYPE,
EccType, sizeof(EccType) );
Csm_KeySetValid(MyEccKeyId);
    
```

#### 7.2.2.4 Redirection of Input and/or Output of Crypto Jobs

**[SWS\_Csm\_91013]** [The input and/or output data of a job can be re-directed to a key element. Which input and output value to which key and its key element is re-directed shall be statically configured at compile time and shall not be changed at runtime.

]()

**[SWS\_Csm\_91014]** [If an input or output value of a job is re-directed to a key element (CsmInOutRedirectionRef ECUC\_Csm\_00262 is existing) and the corresponding input or output length value is not set to 0, the job shall not be processed and E\_NOT\_OK shall be returned.

]()

**[SWS\_Csm\_91015]** [If input or output redirection is not used for a job element (no CsmInOutRedirectionRef ECUC\_Csm\_00262 is existing), jobRedirectionInfoRef shall be set to NULL\_PTR. If redirection is used element (CsmInOutRedirectionRef ECUC\_Csm\_00262 is existing) the jobRedirectionInfoRef shall point to a structure of Crypto\_JobRedirectionInfoType.

]()

**[SWS\_Csm\_91016]** The structure Crypto\_JobRedirectionInfoType contains information which key elements shall be used for redirection. A bit field called redirectionConfig is provided that indicates which input and/or output value is redirected.

The value of redirectionConfig is a bit coded value that is used to indicate, which of the input and output buffers are redirected. If the least significant bit (Bit #0 or 0x01) of redirectionConfig is set the primary input key and its element is redirected and the value of inputKeyId and inputKeyElementId must indicate the element that is used for input buffer instead of the inputPtr and its length. If Bit #1 is set, the secondaryInputBuffer is redirected to the secondary input key is set and the key and

key elements must be set, and Bit #2 is used for the tertiary input key. Bit #3 is reserved for future use.

If Bit #4 is set the outputPtr is redirected to the output key element of the output key. Bit #5 indicates the redirection of the secondary output buffer to the secondary key and its key element. If a bit is set to 0 the input or output shall not be redirected to the associated Key Element.

Example: A value of redirectionConfig of "00110001" indicates that the input should be gathered from the inputKeyElement of inputKeyId and that the output buffer and secondary output buffer shall be redirected to the outputKeyElement of outputKeyId and secondaryOutputKeyElement of secondaryOutputKeyId.

]()

## 7.3 Error Classification

### 7.3.1 Development Errors

#### [SWS\_Csm\_91004][Development Error Types

| Type of error   | Related error code    | Value [hex] |
|---|-----------------------|-------------|
| API request called with invalid parameter (Nullpointer)                 | CSM_E_PARAM_POINTER   | 0x01        |
| Csm Configuration ID 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        |
| API request called with invalid processing mode                         | CSM_E_PROCESSING_MODE | 0x08        |
| Mismatch between the called API request and the service type of the job | CSM_E_SERVICE_TYPE    | 0x09        |

](SRS\_CryptoStack\_00086)

### 7.3.2 Runtime Errors

#### [SWS\_Csm\_01089][Runtime Error Types

| Type of error | Related error code | Value [hex] |
|---------------|--------------------|-------------|
| Queue overrun | CSM_E_QUEUE_FULL   | 0x01        |

](SRS\_CryptoStack\_00086)

### 7.3.3 Transient Faults

There are no transient faults.

### 7.3.4 Production Errors

There are no production errors.

### 7.3.5 Extended Production Errors

There are no extended production errors.

## 7.4 Error detection

**[SWS\_Csm\_91008]** [ While the CSM is not initialized and any function of the CSM API is called, except of `CSM_Init()` and `Csm_GetVersionInfo()`, the operation shall not be performed and `CSM_E_UNINIT` shall be reported to the DET when `CsmDevErrorDetect` is true.

]()

**[SWS\_Csm\_91009]** [If a pointer to null is passed to an API function and the corresponding input or output data are not re-directed to a key element, the operation shall not be performed and `CSM_E_PARAM_POINTER` shall be reported to the DET when `CsmDevErrorDetect` is true.

]()

**[SWS\_Csm\_91011]** [If a CSM API with a ID handle in its interface is called and the ID handle 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.

]()

**[SWS\_Csm\_01091]** [If a CSM API with a job handle (called `jobId`) in its interface is called and the `Crypto_ServiceInfoType` of the job does not match the requested service, the operation shall not be performed and `CSM_E_SERVICE_TYPE` shall be reported to the DET when `CsmDevErrorDetect` is true.

](SRS\_CryptoStack\_00087)

**[SWS\_Csm\_01088]** [If a CSM job needs to be queued and the queue is full, the runtime error `CSM_E_QUEUE_FULL` shall be reported to the DET.

](SRS\_CryptoStack\_00087)

Note: The indication of a queue overrun is logged as runtime error.



## 8 API Specification

### 8.1 Imported types

[SWS\_Csm\_00068] [Only the standard AUTOSAR types provided by Std\_Types.h shall be imported.

]()

### 8.2 Type Definitions

#### 8.2.1 Extension to Std\_ReturnType

[SWS\_Csm\_91043][

|                      |  |      |  |
|----------------------|--|------|--|
| <b>Range</b>         | CRYPTO_E_BUSY  | 0x02 | The service request failed because the service is still busy                               |
|                      | CRYPTO_E_ENTROPY_EXHAUSTED                               | 0x04 | The service request failed because the entropy of the random number generator is exhausted |
|                      | CRYPTO_E_KEY_READ_FAIL                                   | 0x06 | The service request failed because read access was denied                                  |
|                      | CRYPTO_E_KEY_WRITE_FAIL                                  | 0x07 | The service request failed because the writing access failed                               |
|                      | CRYPTO_E_KEY_NOT_AVAILABLE                               | 0x08 | The service request failed because the key is not available                                |
|                      | CRYPTO_E_KEY_NOT_VALID                                   | 0x09 | The service request failed because the key is invalid.                                     |
|                      | CRYPTO_E_KEY_SIZE_MISMATCH                               | 0x0A | The service request failed because the key size does not match.                            |
|                      | CRYPTO_E_JOB_CANCELED                                    | 0x0C | The service request failed because the Job has been canceled.                              |
|                      | CRYPTO_E_KEY_EMPTY                                       | 0x0D | The service request failed because of uninitialized source key element.                    |
| <b>Description</b>   | Overlaid return value of Std_ReturnType for Cryptostack. |      |  |
| <b>Available via</b> | Crypto_GeneralTypes.h                                    |      |  |

](SRS\_CryptoStack\_00095)

#### 8.2.2 Csm\_ConfigType

[SWS\_Csm\_01085][

|             |                |
|-------------|----------------|
| <b>Name</b> | Csm_ConfigType |
|-------------|----------------|

|                      |  |   |
|----------------------|--|---|
| <b>Kind</b>          | Structure                                  |   |
| <b>Elements</b>      | <b>Type</b>                                | --  |
|                      | <b>Comment</b>                             | The content of the configuration data structure is implementation specific. |
| <b>Description</b>   | Configuration data structure of Csm module |   |
| <b>Available via</b> | Csm.h                                      |   |

](SWS\_BSW\_00216)

### 8.2.3 Crypto\_AlgorithmFamilyType

[SWS\_Csm\_01047]

|              |                             |      |                             |
|--------------|-----------------------------|------|-----------------------------|
| <b>Name</b>  | Crypto_AlgorithmFamilyType  |      |                             |
| <b>Kind</b>  | Enumeration                 |      |                             |
| <b>Range</b> | CRYPTO_ALGOFAM_NOT_SET      | 0x00 | Algorithm family is not set |
|              | CRYPTO_ALGOFAM_SHA1         | 0x01 | SHA1 hash                   |
|              | CRYPTO_ALGOFAM_SHA2_224     | 0x02 | SHA2-224 hash               |
|              | CRYPTO_ALGOFAM_SHA2_256     | 0x03 | SHA2-256 hash               |
|              | CRYPTO_ALGOFAM_SHA2_384     | 0x04 | SHA2-384 hash               |
|              | CRYPTO_ALGOFAM_SHA2_512     | 0x05 | SHA2-512 hash               |
|              | CRYPTO_ALGOFAM_SHA2_512_224 | 0x06 | SHA2-512/224 hash           |
|              | CRYPTO_ALGOFAM_SHA2_512_256 | 0x07 | SHA2-512/256 hash           |
|              | CRYPTO_ALGOFAM_SHA3_224     | 0x08 | SHA3-224 hash               |
|              | CRYPTO_ALGOFAM_SHA3_256     | 0x09 | SHA3-256 hash               |
|              | CRYPTO_ALGOFAM_SHA3_384     | 0x0a | SHA3-384 hash               |
|              | CRYPTO_ALGOFAM_SHA3_512     | 0x0b | SHA3-512 hash               |

|                                     |      |   |
|-------------------------------------|------|---|
| CRYPTO_ALGOFAM_SHAKE128             | 0x0c | SHAKE128 hash   |
| CRYPTO_ALGOFAM_SHAKE256             | 0x0d | SHAKE256 hash   |
| CRYPTO_ALGOFAM_RIPEMD160            | 0x0e | RIPEMD hash   |
| CRYPTO_ALGOFAM_BLAKE_1_256          | 0x0f | BLAKE-1-256 hash  |
| CRYPTO_ALGOFAM_BLAKE_1_512          | 0x10 | BLAKE-1-512 hash  |
| CRYPTO_ALGOFAM_BLAKE_2s_256         | 0x11 | BLAKE-2s-256 hash   |
| CRYPTO_ALGOFAM_BLAKE_2s_512         | 0x12 | BLAKE-2s-512 hash   |
| CRYPTO_ALGOFAM_3DES                 | 0x13 | 3DES cipher   |
| CRYPTO_ALGOFAM_AES                  | 0x14 | AES cipher  |
| CRYPTO_ALGOFAM_CHACHA               | 0x15 | ChaCha cipher   |
| CRYPTO_ALGOFAM_RSA                  | 0x16 | RSA cipher  |
| CRYPTO_ALGOFAM_ED25519              | 0x17 | ED25519 elliptic curve  |
| CRYPTO_ALGOFAM_BRAINPOOL            | 0x18 | Brainpool elliptic curve  |
| CRYPTO_ALGOFAM_ECCNIST              | 0x19 | NIST ECC elliptic curves  |
| CRYPTO_ALGOFAM_RNG                  | 0x1b | Random Number Generator   |
| CRYPTO_ALGOFAM_SIPHASH              | 0x1c | SipHash   |
| CRYPTO_ALGOFAM_ECCANSI              | 0x1e | Elliptic curve according to ANSI X9.62  |
| CRYPTO_ALGOFAM_ECCSEC               | 0x1f | Elliptic curve according to SECG  |
| CRYPTO_ALGOFAM_DRBG                 | 0x20 | Random number generator according to NIST SP800-90A   |
| CRYPTO_ALGOFAM_FIPS186              | 0x21 | Random number generator according to FIPS 186.  |
| CRYPTO_ALGOFAM_PADDING_PKCS7        | 0x22 | Cipher padding according to PKCS.7  |
| CRYPTO_ALGOFAM_PADDING_ONEWITHZEROS | 0x23 | Cipher padding mode. Fill/verify data with 0, but first bit after the data is 1. Eg. "DATA" & |

|                      |                                      |      |  |
|----------------------|--------------------------------------|------|--|
|                      |                                      |      | 0x80 & 0x00...                           |
|                      | CRYPTO_ALGOFAM_PBKDF2                | 0x24 | Password-Based Key Derivation Function 2 |
|                      | CRYPTO_ALGOFAM_KDFX963               | 0x25 | ANSI X9.63 Public Key Cryptography       |
|                      | CRYPTO_ALGOFAM_DH                    | 0x26 | Diffie-Hellman                           |
|                      | CRYPTO_ALGOFAM_CUSTOM                | 0xff | Custom algorithm family                  |
| <b>Description</b>   | Enumeration of the algorithm family. |      |  |
| <b>Available via</b> | Crypto_GeneralTypes.h                |      |  |

]()

## 8.2.4 Crypto\_AlgorithmModeType

[SWS\_Csm\_01048]

|                         |                                   |                         |   |
|-------------------------|-----------------------------------|-------------------------|---|
| <b>Name</b>             | Crypto_AlgorithmModeType          |                         |   |
| <b>Kind</b>             | Enumeration                       |                         |   |
| <b>Range</b>            | CRYPTO_ALGOMODE_NOT_SET           | 0x00                    | Algorithm key is not set  |
|                         | CRYPTO_ALGOMODE_ECB               | 0x01                    | Blockmode: Electronic Code Book                                     |
|                         | CRYPTO_ALGOMODE_CBC               | 0x02                    | Blockmode: Cipher Block Chaining                                    |
|                         | CRYPTO_ALGOMODE_CFB               | 0x03                    | Blockmode: Cipher Feedback Mode                                     |
|                         | CRYPTO_ALGOMODE_OFB               | 0x04                    | Blockmode: Output Feedback Mode                                     |
|                         | CRYPTO_ALGOMODE_CTR               | 0x05                    | Blockmode: Counter Modex  |
|                         | CRYPTO_ALGOMODE_GCM               | 0x06                    | Blockmode: Galois/Counter Mode                                      |
|                         | CRYPTO_ALGOMODE_XTS               | 0x07                    | XOR-encryption-based tweaked-codebook mode with ciphertext stealing |
|                         | CRYPTO_ALGOMODE_RSAES_OAEP        | 0x08                    | RSA Optimal Asymmetric Encryption Padding                           |
|                         | CRYPTO_ALGOMODE_RSAES_PKCS1_v1_5  | 0x09                    | RSA encryption/decryption with PKCS#1 v1.5 padding                  |
|                         | CRYPTO_ALGOMODE_RSASSA_PSS        | 0x0a                    | RSA Probabilistic Signature Scheme                                  |
|                         | CRYPTO_ALGOMODE_RSASSA_PKCS1_v1_5 | 0x0b                    | RSA signature with PKCS#1 v1.5                                      |
| CRYPTO_ALGOMODE_8ROUNDS | 0x0c                              | 8 rounds (e.g. ChaCha8) |   |

|                      |                                   |      |  |
|----------------------|-----------------------------------|------|--|
|                      | CRYPTO_ALGOMODE_12ROUNDS          | 0x0d | 12 rounds (e.g. ChaCha12)                        |
|                      | CRYPTO_ALGOMODE_20ROUNDS          | 0x0e | 20 rounds (e.g. ChaCha20)                        |
|                      | CRYPTO_ALGOMODE_HMAC              | 0x0f | Hashed-based MAC                                 |
|                      | CRYPTO_ALGOMODE_CMAC              | 0x10 | Cipher-based MAC                                 |
|                      | CRYPTO_ALGOMODE_GMAC              | 0x11 | Galois MAC                                       |
|                      | CRYPTO_ALGOMODE_CTRDRBG           | 0x12 | Counter-based Deterministic Random Bit Generator |
|                      | CRYPTO_ALGOMODE_SIPHASH_2_4       | 0x13 | Siphash-2-4                                      |
|                      | CRYPTO_ALGOMODE_SIPHASH_4_8       | 0x14 | Siphash-4-8                                      |
|                      | CRYPTO_ALGOMODE_PXXR1             | 0x15 | ANSI R1 Curve                                    |
|                      | CRYPTO_ALGOMODE_CUSTOM            | 0xff | Custom algorithm mode                            |
| <b>Description</b>   | Enumeration of the algorithm mode |      |  |
| <b>Available via</b> | Crypto_GeneralTypes.h             |      |  |

]()

### 8.2.5 Crypto\_InputOutputRedirectionConfigType

[SWS\_Csm\_91024]

|                      |  |      |    |
|----------------------|--|------|----|
| <b>Name</b>          | Crypto_InputOutputRedirectionConfigType  |      |    |
| <b>Kind</b>          | Enumeration  |      |    |
| <b>Range</b>         | CRYPTO_REDIRECT_CONFIG_PRIMARY_INPUT   | 0x01 | -- |
|                      | CRYPTO_REDIRECT_CONFIG_SECONDARY_INPUT   | 0x02 | -- |
|                      | CRYPTO_REDIRECT_CONFIG_TERTIARY_INPUT  | 0x04 | -- |
|                      | CRYPTO_REDIRECT_CONFIG_PRIMARY_OUTPUT  | 0x10 | -- |
|                      | CRYPTO_REDIRECT_CONFIG_SECONDARY_OUTPUT  | 0x20 | -- |
| <b>Description</b>   | Defines which of the input/output parameters are re-directed to a key element. The values can be combined to define a bit field. |      |    |
| <b>Available via</b> | Crypto_GeneralTypes.h  |      |    |

]()

## 8.2.6 Crypto\_JobType

### [SWS\_Csm\_01013]

|                   |  |  |
|-------------------|--|--|
| <b>Name</b>       | Crypto_JobType   |  |
| <b>Kind</b>       | Structure  |  |
| <b>Elements</b>   | jobId  |  |
|                   | <b>Type</b>  | uint32   |
|                   | <b>Comment</b>   | Identifier for the job structure.  |
|                   | jobState   |  |
|                   | <b>Type</b>  | Crypto_JobStateType  |
|                   | <b>Comment</b>   | Determines the current job state.  |
|                   | jobPrimitiveInputOutput  |  |
|                   | <b>Type</b>  | Crypto_JobPrimitiveInputOutputType   |
|                   | <b>Comment</b>   | Structure containing input and output information depending on the job and the crypto primitive.         |
|                   | jobPrimitiveInfo   |  |
|                   | <b>Type</b>  | const Crypto_JobPrimitiveInfoType*   |
|                   | <b>Comment</b>   | Pointer to a structure containing further information which depends on the job and the crypto primitive. |
|                   | jobInfo  |  |
|                   | <b>Type</b>  | const Crypto_JobInfoType*  |
|                   | <b>Comment</b>   | Pointer to a structure containing further information which depends on the job and the crypto primitive. |
|                   | cryptoKeyld  |  |
|                   | <b>Type</b>  | uint32   |
|                   | <b>Comment</b>   | Identifier of the Crypto Driver key. The identifier shall be written by the Crypto Interface.            |
|                   | jobRedirectionInfoRef  |  |
|                   | <b>Type</b>  | Crypto_JobRedirectionInfoType*   |
| <b>Comment</b>    | Pointer to a structure containing further information on the usage of keys as input and output for jobs. |  |
| targetCryptoKeyld |  |  |
| <b>Type</b>       | uint32   |  |
| <b>Comment</b>    | Target identifier of the Crypto Driver key. The identifier shall be written by the Crypto Interface.     |  |

|                      |  |
|----------------------|--|
| <b>Description</b>   | Structure which contains further information, which depends on the job and the crypto primitive. |
| <b>Available via</b> | Crypto_GeneralTypes.h  |

]()

### 8.2.7 Crypto\_JobStateType

[SWS\_Csm\_01028]

|                      |                                       |      |   |
|----------------------|---------------------------------------|------|---|
| <b>Name</b>          | Crypto_JobStateType                   |      |   |
| <b>Kind</b>          | Enumeration                           |      |   |
| <b>Range</b>         | CRYPTO_JOBSTATE_IDLE                  | 0x00 | Job is in the state "idle". This state is reached after Csm_Init() or when the "Finish" state is finished.  |
|                      | CRYPTO_JOBSTATE_ACTIVE                | 0x01 | Job is in the state "active". There was already some input or there are intermediate results. This state is reached, when the "update" or "start" operation finishes. |
| <b>Description</b>   | Enumeration of the current job state. |      |   |
| <b>Available via</b> | Crypto_GeneralTypes.h                 |      |   |

]()

### 8.2.8 Crypto\_JobPrimitiveInputOutputType

[SWS\_Csm\_01009]

|                 |                                    |   |  |
|-----------------|------------------------------------|---|--|
| <b>Name</b>     | Crypto_JobPrimitiveInputOutputType |   |  |
| <b>Kind</b>     | Structure                          |   |  |
| <b>Elements</b> | inputPtr                           |   |  |
|                 | <b>Type</b>                        | const uint8*  |  |
|                 | <b>Comment</b>                     | Pointer to the input data.  |  |
|                 | inputLength                        |   |  |
|                 | <b>Type</b>                        | uint32  |  |
|                 | <b>Comment</b>                     | Contains the input length in bytes.                                   |  |
|                 | secondaryInputPtr                  |   |  |
|                 | <b>Type</b>                        | const uint8*  |  |
|                 | <b>Comment</b>                     | Pointer to the secondary input data (for MacVerify, SignatureVerify). |  |
|                 | secondaryInputLength               |   |  |

|                |   |   |
|----------------|---|---|
|                | <b>Type</b>   | uint32  |
|                | <b>Comment</b>  | Contains the secondary input length in bits or bytes, depending on the requested service. |
|                | tertiaryInputPtr                                      |   |
|                | <b>Type</b>   | const uint8*  |
|                | <b>Comment</b>  | Pointer to the tertiary input data (for MacVerify, SignatureVerify).                      |
|                | tertiaryInputLength                                   |   |
|                | <b>Type</b>   | uint32  |
|                | <b>Comment</b>  | Contains the tertiary input length in bytes.  |
|                | outputPtr   |   |
|                | <b>Type</b>   | uint8*  |
|                | <b>Comment</b>  | Pointer to the output data.   |
|                | outputLengthPtr                                       |   |
|                | <b>Type</b>   | uint32*   |
|                | <b>Comment</b>  | Holds a pointer to a memory location containing the output length in bytes.               |
|                | secondaryOutputPtr                                    |   |
|                | <b>Type</b>   | uint8*  |
|                | <b>Comment</b>  | Pointer to the secondary output data.   |
|                | secondaryOutputLengthPtr                              |   |
|                | <b>Type</b>   | uint32*   |
|                | <b>Comment</b>  | Holds a pointer to a memory location containing the secondary output length in bytes.     |
|                | input64   |   |
|                | <b>Type</b>   | uint64  |
|                | <b>Comment</b>  | versatile input parameter   |
|                | verifyPtr   |   |
|                | <b>Type</b>   | Crypto_VerifyResultType*  |
|                | <b>Comment</b>  | Output pointer to a memory location holding a Crypto_VerifyResultType                     |
|                | output64Ptr   |   |
|                | <b>Type</b>   | uint64*   |
| <b>Comment</b> | Output pointer to a memory location holding a uint64. |   |



|                      |  |   |
|----------------------|--|---|
|                      | mode   |   |
|                      | <b>Type</b>  | Crypto_OperationModeType                                  |
|                      | <b>Comment</b>   | Indicator of the mode(s)/operation(s) to be performed     |
|                      | cryIfKeyId   |   |
|                      | <b>Type</b>  | uint32  |
|                      | <b>Comment</b>   | Holds the CryIf key id for key operation services.        |
|                      | targetCryIfKeyId   |   |
|                      | <b>Type</b>  | uint32  |
|                      | <b>Comment</b>   | Holds the target CryIf key id for key operation services. |
| <b>Description</b>   | Structure which contains input and output information depending on the job and the crypto primitive. |   |
| <b>Available via</b> | Crypto_GeneralTypes.h  |   |

]()

### 8.2.9 Crypto\_JobInfoType

[SWS\_Csm\_01010]

|                      |   |   |
|----------------------|---|---|
| <b>Name</b>          | Crypto_JobInfoType  |   |
| <b>Kind</b>          | Structure   |   |
| <b>Elements</b>      | jobId   |   |
|                      | <b>Type</b>   | const uint32  |
|                      | <b>Comment</b>  | The family of the algorithm   |
|                      | jobPriority   |   |
|                      | <b>Type</b>   | const uint32  |
|                      | <b>Comment</b>  | Specifies the importance of the job (the higher, the more important). |
| <b>Description</b>   | Structure which contains job information (job ID and job priority). |   |
| <b>Available via</b> | Crypto_GeneralTypes.h   |   |

](SRS\_CryptoStack\_00102)

### 8.2.10 Crypto\_JobPrimitiveInfoType

[SWS\_Csm\_01012]

|             |                             |
|-------------|-----------------------------|
| <b>Name</b> | Crypto_JobPrimitiveInfoType |
|-------------|-----------------------------|

|                      |  |   |  |
|----------------------|--|---|--|
| <b>Kind</b>          | Structure  |   |  |
| <b>Elements</b>      | callbackId   |   |  |
|                      | <b>Type</b>  | uint32  |  |
|                      | <b>Comment</b>   | Internal identifier of the callback function, to be called by Csm, if the configured service is finished. |  |
|                      | primitiveInfo  |   |  |
|                      | <b>Type</b>  | const Crypto_PrimitiveInfoType*   |  |
|                      | <b>Comment</b>   | Pointer to a structure containing further configuration of the crypto primitives                          |  |
|                      | cryIfKeyId   |   |  |
|                      | <b>Type</b>  | uint32  |  |
|                      | <b>Comment</b>   | Identifier of the CryIf key.  |  |
|                      | processingType   |   |  |
|                      | <b>Type</b>  | Crypto_ProcessingType   |  |
|                      | <b>Comment</b>   | Determines the synchronous or asynchronous behavior.  |  |
| <b>Description</b>   | Structure which contains further information, which depends on the job and the crypto primitive. |   |  |
| <b>Available via</b> | Crypto_GeneralTypes.h  |   |  |

](SRS\_CryptoStack\_00008)

### 8.2.11 Crypto\_ServiceInfoType

[SWS\_Csm\_01031]

|              |                          |      |                           |
|--------------|--------------------------|------|---------------------------|
| <b>Name</b>  | Crypto_ServiceInfoType   |      |                           |
| <b>Kind</b>  | Enumeration              |      |                           |
| <b>Range</b> | CRYPTO_HASH              | 0x00 | Hash Service              |
|              | CRYPTO_MACGENERATE       | 0x01 | MacGenerate Service       |
|              | CRYPTO_MACVERIFY         | 0x02 | MacVerify Service         |
|              | CRYPTO_ENCRYPT           | 0x03 | Encrypt Service           |
|              | CRYPTO_DECRYPT           | 0x04 | Decrypt Service           |
|              | CRYPTO_AEADENCRYPT       | 0x05 | AEADEncrypt Service       |
|              | CRYPTO_AEADDECRYPT       | 0x06 | AEADDecrypt Service       |
|              | CRYPTO_SIGNATUREGENERATE | 0x07 | SignatureGenerate Service |

|                      |   |      |                               |
|----------------------|---|------|-------------------------------|
|                      | CRYPTO_SIGNATUREVERIFY                  | 0x08 | SignatureVerify Service       |
|                      | CRYPTO_RANDOMGENERATE                   | 0x0B | RandomGenerate Service        |
|                      | CRYPTO_RANDOMSEED                       | 0x0C | RandomSeed Service            |
|                      | CRYPTO_KEYGENERATE                      | 0x0D | KeyGenerate Service           |
|                      | CRYPTO_KEYDERIVE                        | 0x0E | KeyDerive Service             |
|                      | CRYPTO_KEYEXCHANGEALCPUBVAL             | 0x0F | KeyExchangeCalcPubVal Service |
|                      | CRYPTO_KEYEXCHANGEALCSECRET             | 0x10 | KeyExchangeCalcSecret Service |
|                      | CRYPTO_KEYSETVALID                      | 0x13 | KeySetValid Service           |
| <b>Description</b>   | Enumeration of the kind of the service. |      |                               |
| <b>Available via</b> | Crypto_GeneralTypes.h                   |      |                               |

l()

### 8.2.12 Crypto\_JobRedirectionInfoType

[SWS\_Csm\_91026]

|                 |                               |  |
|-----------------|-------------------------------|--|
| <b>Name</b>     | Crypto_JobRedirectionInfoType |  |
| <b>Kind</b>     | Structure                     |  |
| <b>Elements</b> | redirectionConfig             |  |
|                 | <b>Type</b>                   | uint8  |
|                 | <b>Comment</b>                | Bit structure which indicates which buffer shall be redirected to a key element. Values from Crypto_InputOutputRedirectionConfigType can be used and combined with unary OR operation. |
|                 | inputKeyld                    |  |
|                 | <b>Type</b>                   | uint32   |
|                 | <b>Comment</b>                | Identifier of the key which shall be used as input   |
|                 | inputKeyElementld             |  |
|                 | <b>Type</b>                   | uint32   |
|                 | <b>Comment</b>                | Identifier of the key element which shall be used as input   |
|                 | secondaryInputKeyld           |  |
|                 | <b>Type</b>                   | uint32   |
|                 | <b>Comment</b>                | Identifier of the key which shall be used as secondary input   |

|                      |   |
|----------------------|---|
|                      | secondaryInputKeyElementId  |
| <b>Type</b>          | uint32  |
| <b>Comment</b>       | Identifier of the key element which shall be used as secondary input  |
|                      | tertiaryInputKeyId  |
| <b>Type</b>          | uint32  |
| <b>Comment</b>       | Identifier of the key which shall be used as tertiary input   |
|                      | tertiaryInputKeyElementId   |
| <b>Type</b>          | uint32  |
| <b>Comment</b>       | Identifier of the key element which shall be used as tertiary input   |
|                      | outputKeyId   |
| <b>Type</b>          | uint32  |
| <b>Comment</b>       | Identifier of the key which shall be used as output   |
|                      | outputKeyElementId  |
| <b>Type</b>          | uint32  |
| <b>Comment</b>       | Identifier of the key element which shall be used as output   |
|                      | secondaryOutputKeyId  |
| <b>Type</b>          | uint32  |
| <b>Comment</b>       | Identifier of the key which shall be used as secondary output   |
|                      | secondaryOutputKeyElementId   |
| <b>Type</b>          | uint32  |
| <b>Comment</b>       | Identifier of the key element which shall be used as secondary output   |
| <b>Description</b>   | Structure which holds the identifiers of the keys and key elements which shall be used as input and output for a job and a bit structure which indicates which buffers shall be redirected to those key elements. |
| <b>Available via</b> | Crypto_GeneralTypes.h   |

]()

### 8.2.13 Crypto\_AlgorithmInfoType

[SWS\_Csm\_01008]

|             |                          |
|-------------|--------------------------|
| <b>Name</b> | Crypto_AlgorithmInfoType |
| <b>Kind</b> | Structure                |

|                      |   |   |  |
|----------------------|---|---|--|
| <b>Elements</b>      | family  |   |  |
|                      | <b>Type</b>   | Crypto_AlgorithmFamilyType                            |  |
|                      | <b>Comment</b>  | The family of the algorithm                           |  |
|                      | secondaryFamily   |   |  |
|                      | <b>Type</b>   | Crypto_AlgorithmFamilyType                            |  |
|                      | <b>Comment</b>  | The secondary family of the algorithm                 |  |
|                      | keyLength   |   |  |
|                      | <b>Type</b>   | uint32  |  |
|                      | <b>Comment</b>  | The key length in bits to be used with that algorithm |  |
|                      | mode  |   |  |
|                      | <b>Type</b>   | Crypto_AlgorithmModeType                              |  |
|                      | <b>Comment</b>  | The operation mode to be used with that algorithm     |  |
| <b>Description</b>   | Structure which determines the exact algorithm. Note, not every algorithm needs to specify all fields. AUTOSAR shall only allow valid combinations. |   |  |
| <b>Available via</b> | Crypto_GeneralTypes.h   |   |  |

]()

### 8.2.14 Crypto\_ProcessingType

[SWS\_Csm\_01049]

|                      |                                     |      |                             |
|----------------------|-------------------------------------|------|-----------------------------|
| <b>Name</b>          | Crypto_ProcessingType               |      |                             |
| <b>Kind</b>          | Enumeration                         |      |                             |
| <b>Range</b>         | CRYPTO_PROCESSING_ASYNC             | 0x00 | Asynchronous job processing |
|                      | CRYPTO_PROCESSING_SYNC              | 0x01 | Synchronous job processing  |
| <b>Description</b>   | Enumeration of the processing type. |      |                             |
| <b>Available via</b> | Crypto_GeneralTypes.h               |      |                             |

] (SRS\_CryptoStack\_00100, SRS\_CryptoStack\_00101)

### 8.2.15 Crypto\_PrimitiveInfoType

[SWS\_Csm\_01011]

|             |                          |
|-------------|--------------------------|
| <b>Name</b> | Crypto_PrimitiveInfoType |
| <b>Kind</b> | Structure                |

|                      |  |   |  |
|----------------------|--|---|--|
| <b>Elements</b>      | resultLength   |   |  |
|                      | <b>Type</b>  | const uint32  |  |
|                      | <b>Comment</b>   | Contains the result length in bytes.                |  |
|                      | service  |   |  |
|                      | <b>Type</b>  | const Crypto_ServiceInfoType                        |  |
|                      | <b>Comment</b>   | Contains the enum of the used service, e.g. Encrypt |  |
|                      | algorithm  |   |  |
|                      | <b>Type</b>  | const Crypto_AlgorithmInfoType                      |  |
|                      | <b>Comment</b>   | Contains the information of the used algorithm      |  |
| <b>Description</b>   | Structure which contains basic information about the crypto primitive. |   |  |
| <b>Available via</b> | Crypto_GeneralTypes.h  |   |  |

]()

### 8.2.16 Csm\_ConfigIdType

[SWS\_Csm\_00691]

|                      |   |    |    |
|----------------------|---|----|----|
| <b>Name</b>          | Csm_ConfigIdType  |    |    |
| <b>Kind</b>          | Type  |    |    |
| <b>Derived from</b>  | uint16  |    |    |
| <b>Range</b>         | 0..65535  | -- | -- |
| <b>Description</b>   | Identification of a CSM service configuration via a numeric identifier, that is unique within a service. The name of a CSM service configuration, i.e. the name of the container Csm_<Service>Config, shall serve as a symbolic name for this parameter |    |    |
| <b>Available via</b> | Csm.h   |    |    |

](SRS\_Csm\_00066)

## 8.3 Function Definitions

[SWS\_Csm\_00478] [All functions need not to be reentrant. For behavior in case of a reentrant call see **SWS\_Csm\_00017**.

]()

### 8.3.1 General Interface

#### 8.3.1.1 Csm\_Init

[SWS\_Csm\_00646]

|                           |  |   |
|---------------------------|--|---|
| <b>Service Name</b>       | Csm_Init   |   |
| <b>Syntax</b>             | <pre>void Csm_Init (     const Csm_ConfigType* configPtr )</pre> |   |
| <b>Service ID [hex]</b>   | 0x00   |   |
| <b>Sync/Async</b>         | Synchronous  |   |
| <b>Reentrancy</b>         | Non Reentrant  |   |
| <b>Parameters (in)</b>    | configPtr  | Pointer to a selected configuration structure |
| <b>Parameters (inout)</b> | None   |   |
| <b>Parameters (out)</b>   | None   |   |
| <b>Return value</b>       | None   |   |
| <b>Description</b>        | Initializes the CSM module.                                      |   |
| <b>Available via</b>      | Csm.h  |   |

](SRS\_BSW\_00101, SRS\_BSW\_00358, SRS\_BSW\_00414)

[SWS\_Csm\_00186] [The Configuration pointer `configPtr` shall always have a null pointer value.

](SWS\_BSW\_00050)

The Configuration pointer `configPtr` is currently not used and shall therefore be set null pointer value.

[SWS\_Csm\_00659] [If the initialization of the CSM module fails, the CSM shall report `CSM_E_INIT_FAILED` to the DET when `CsmDevErrorDetect` is true.

](

#### 8.3.1.2 Csm\_GetVersionInfo

[SWS\_Csm\_00705]

|                         |   |  |
|-------------------------|---|--|
| <b>Service Name</b>     | Csm_GetVersionInfo  |  |
| <b>Syntax</b>           | <pre>void Csm_GetVersionInfo (     Std_VersionInfoType* versioninfo )</pre> |  |
| <b>Service ID [hex]</b> | 0x3b  |  |
| <b>Sync/Async</b>       | Synchronous   |  |

|                           |   |   |
|---------------------------|---|---|
| <b>Reentrancy</b>         | Reentrant                                       |   |
| <b>Parameters (in)</b>    | None  |   |
| <b>Parameters (inout)</b> | None  |   |
| <b>Parameters (out)</b>   | versioninfo                                     | Pointer to where to store the version information of this module. |
| <b>Return value</b>       | None  |   |
| <b>Description</b>        | Returns the version information of this module. |   |
| <b>Available via</b>      | Csm.h   |   |

](SRS\_BSW\_00407)

### 8.3.2 Hash Interface

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the hash value, such that an accidental or intentional change to the data will change the hash value. Main properties of hash functions are that it is infeasible to find a message that has a given hash or to find two different messages with the same hash.

#### 8.3.2.1 Csm\_Hash

[SWS\_Csm\_00980][

|                         |  |  |
|-------------------------|--|--|
| <b>Service Name</b>     | Csm_Hash   |  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_Hash (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* dataPtr,     uint32 dataLength,     uint8* resultPtr,     uint32* resultLengthPtr )</pre> |  |
| <b>Service ID [hex]</b> | 0x5d   |  |
| <b>Sync/Async</b>       | Asynchronous or Async, depending on the job configuration  |  |
| <b>Reentrancy</b>       | Reentrant  |  |
| <b>Parameters (in)</b>  | jobId  | Holds the identifier of the job using the CSM service.                 |
|                         | mode   | Indicates which operation mode(s) to perform.                          |
|                         | dataPtr  | Contains the pointer to the data for which the hash shall be computed. |
|                         | data Length  | Contains the number of bytes to be hashed.                             |



|                           |  |  |
|---------------------------|--|--|
| <b>Parameters (inout)</b> | result<br>LengthPtr  | 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 resultPtr. When the request has finished, the actual length of the returned value shall be stored. |
| <b>Parameters (out)</b>   | resultPtr  | Contains the pointer to the data where the hash value shall be stored.   |
| <b>Return value</b>       | Std_-<br>Return-<br>Type   | E_OK: Request successful<br>E_NOT_OK: Request failed   |
| <b>Description</b>        | Uses the given data to perform the hash calculation and stores the hash. |  |
| <b>Available via</b>      | Csm.h  |  |

](SRS\_CryptoStack\_00024)

### 8.3.3 MAC interface

A message authentication code (MAC) is a short piece of information used to authenticate a message. A MAC algorithm accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

#### 8.3.3.1 Csm\_MacGenerate

[SWS\_Csm\_00982][

|                         |   |   |
|-------------------------|---|---|
| <b>Service Name</b>     | Csm_MacGenerate   |   |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_MacGenerate (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* dataPtr,     uint32 dataLength,     uint8* macPtr,     uint32* macLengthPtr )</pre> |   |
| <b>Service ID [hex]</b> | 0x60  |   |
| <b>Sync/Async</b>       | Asynchronous or Async, dependent on the job configuration   |   |
| <b>Reentrancy</b>       | Reentrant   |   |
| <b>Parameters (in)</b>  | jobId   | Holds the identifier of the job using the CSM service.                |
|                         | mode  | Indicates which operation mode(s) to perform.                         |
|                         | dataPtr   | Contains the pointer to the data for which the MAC shall be computed. |

|                           |  |  |
|---------------------------|--|--|
|                           | data Length  | Contains the number of bytes to be hashed.   |
| <b>Parameters (inout)</b> | mac LengthPtr  | 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.  |
| <b>Parameters (out)</b>   | macPtr   | Contains the pointer to the data where the MAC shall be stored.  |
| <b>Return value</b>       | Std_ReturnType   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer. |  |
| <b>Available via</b>      | Csm.h  |  |

](SRS\_CryptoStack\_00022)

### 8.3.3.2 Csm\_MacVerify

[SWS\_Csm\_01050]

|                         |   |  |
|-------------------------|---|--|
| <b>Service Name</b>     | Csm_MacVerify   |  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_MacVerify (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* dataPtr,     uint32 dataLength,     const uint8* macPtr,     const uint32 macLength,     Crypto_VerifyResultType* verifyPtr )</pre> |  |
| <b>Service ID [hex]</b> | 0x61  |  |
| <b>Sync/Async</b>       | Asynchronous or Async, dependend on the job configuration   |  |
| <b>Reentrancy</b>       | Reentrant   |  |
| <b>Parameters (in)</b>  | jobId   | Indicates which operation mode(s) to perform.                          |
|                         | mode  | Indicates which operation mode(s) to perform.                          |
|                         | dataPtr   | Holds a pointer to the data for which the MAC shall be verified.       |
|                         | dataLength  | Contains the number of data bytes for which the MAC shall be verified. |

|                           |  |  |
|---------------------------|--|--|
|                           | macPtr   | Holds a pointer to the MAC to be verified.   |
|                           | macLength  | Contains the MAC length in BITS to be verified.  |
| <b>Parameters (inout)</b> | None   |  |
| <b>Parameters (out)</b>   | verifyPtr  | Holds a pointer to the memory location, which will hold the result of the MAC verification.  |
| <b>Return value</b>       | Std_Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Verifies the given MAC by comparing if the MAC is generated with the given data. |  |
| <b>Available via</b>      | Csm.h  |  |

l()

### 8.3.4 Cipher Interface

The cipher interfaces can be used for symmetrical and asymmetrical encryption or decryption. Furthermore, it is also possible to use these interfaces for compression and decompression, respectively.

#### 8.3.4.1 Csm\_Encrypt

[SWS\_Csm\_00984]

|                         |   |  |
|-------------------------|---|--|
| <b>Service Name</b>     | Csm_Encrypt   |  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_Encrypt (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* dataPtr,     uint32 dataLength,     uint8* resultPtr,     uint32* resultLengthPtr )</pre> |  |
| <b>Service ID [hex]</b> | 0x5e  |  |
| <b>Sync/Async</b>       | Asynchronous or Async, dependend on the job configuration   |  |
| <b>Reentrancy</b>       | Reentrant   |  |
| <b>Parameters</b>       | jobId   | Holds the identifier of the job using the CSM service. |

|                           |  |  |
|---------------------------|--|--|
| <b>(in)</b>               | mode   | Indicates which operation mode(s) to perform.  |
|                           | dataPtr  | Contains the pointer to the data to be encrypted.  |
|                           | data Length  | Contains the number of bytes to encrypt.   |
| <b>Parameters (inout)</b> | result LengthPtr   | Holds a pointer to the memory location in which the output length information is stored in bytes. 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.   |
| <b>Parameters (out)</b>   | resultPtr  | Contains the pointer to the data where the encrypted data shall be stored.   |
| <b>Return value</b>       | Std - Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Encrypts the given data and store the ciphertext in the memory location pointed by the result pointer. |  |
| <b>Available via</b>      | Csm.h  |  |

](SRS\_CryptoStack\_00020, SRS\_CryptoStack\_00021)

In the case of block ciphers, it shall be possible to pass a `dataLength` which is not a multiple of the corresponding block size. The underlying Crypto Driver is responsible for handling these input data.

### 8.3.4.2 Csm\_Decrypt

[SWS\_Csm\_00989]

|                         |   |
|-------------------------|---|
| <b>Service Name</b>     | Csm_Decrypt   |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_Decrypt (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* dataPtr,     uint32 dataLength,     uint8* resultPtr,     uint32* resultLengthPtr )</pre> |
| <b>Service ID [hex]</b> | 0x5f  |
| <b>Sync/Async</b>       | Asynchronous or Async, dependend on the job configuration   |

|                           |   |  |
|---------------------------|---|--|
| <b>Reentrancy</b>         | Reentrant   |  |
| <b>Parameters (in)</b>    | jobId   | Holds the identifier of the job using the CSM service.   |
|                           | mode  | Indicates which operation mode(s) to perform.  |
|                           | dataPtr   | Contains the pointer to the data to be decrypted.  |
|                           | data Length   | Contains the number of bytes to decrypt.   |
| <b>Parameters (inout)</b> | result LengthPtr  | Holds a pointer to the memory location in which the output length information is stored in bytes. 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.   |
| <b>Parameters (out)</b>   | resultPtr   | Contains the pointer to the memory location where the decrypted data shall be stored.  |
| <b>Return value</b>       | Std_-Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Decrypts the given encrypted data and store the decrypted plaintext in the memory location pointed by the result pointer. |  |
| <b>Available via</b>      | Csm.h   |  |

[(SRS\_CryptoStack\_00020, SRS\_CryptoStack\_00021)]

### 8.3.5 Authenticated Encryption with Associated Data (AEAD) Interface

AEAD (also known as Authenticated Encryption) is a block cipher mode of operation which also allows integrity checks (e.g. AES-GCM).

#### 8.3.5.1 Csm\_AEADEncrypt

[SWS\_Csm\_01023]

|                     |  |
|---------------------|--|
| <b>Service Name</b> | Csm_AEADEncrypt  |
| <b>Syntax</b>       | <pre>Std_ReturnType Csm_AEADEncrypt (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* plaintextPtr,     uint32 plaintextLength,     const uint8* associatedDataPtr,     uint32 associatedDataLength,     uint8* ciphertextPtr,</pre> |

|                           |   |  |
|---------------------------|---|--|
|                           | <pre>uint32* ciphertextLengthPtr, uint8* tagPtr, uint32* tagLengthPtr )</pre>   |  |
| <b>Service ID [hex]</b>   | 0x62  |  |
| <b>Sync/Async</b>         | Asynchronous or Async, dependend on the job configuration   |  |
| <b>Reentrancy</b>         | Reentrant   |  |
| <b>Parameters (in)</b>    | jobId   | Holds the identifier of the job using the CSM service.   |
|                           | mode  | Indicates which operation mode(s) to perform.  |
|                           | plaintextPtr  | Contains the pointer to the data to be encrypted.  |
|                           | plaintext Length  | Contains the number of bytes to encrypt.   |
|                           | associated DataPtr  | Contains the pointer to the associated data.   |
|                           | associated DataLength   | Contains the number of bytes of the associated data.   |
| <b>Parameters (inout)</b> | ciphertext LengthPtr  | 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.  |
|                           | 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.   |
| <b>Parameters (out)</b>   | ciphertextPtr   | Contains the pointer to the data where the encrypted data shall be stored.   |
|                           | tagPtr  | Contains the pointer to the data where the Tag shall be stored.  |
| <b>Return value</b>       | Std_Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | 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. |  |
| <b>Available via</b>      | Csm.h   |  |

l()

### 8.3.5.2 Csm\_AEADDecrypt

[SWS\_Csm\_01026]

|                           |   |   |
|---------------------------|---|---|
| <b>Service Name</b>       | Csm_AEADDecrypt   |   |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_AEADDecrypt (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* ciphertextPtr,     uint32 ciphertextLength,     const uint8* associatedDataPtr,     uint32 associatedDataLength,     const uint8* tagPtr,     uint32 tagLength,     uint8* plaintextPtr,     uint32* plaintextLengthPtr,     Crypto_VerifyResultType* verifyPtr )</pre> |   |
| <b>Service ID [hex]</b>   | 0x63  |   |
| <b>Sync/Async</b>         | Asynchronous or Async, dependend on the job configuration   |   |
| <b>Reentrancy</b>         | Reentrant   |   |
| <b>Parameters (in)</b>    | jobId   | Holds the identifier of the job using the CSM service.  |
|                           | mode  | Indicates which operation mode(s) to perform.   |
|                           | ciphertextPtr   | Contains the pointer to the data to be decrypted.   |
|                           | ciphertext Length   | Contains the number of bytes to decrypt.  |
|                           | associated DataPtr  | Contains the pointer to the associated data.  |
|                           | associated DataLength   | Contains the length in bytes of the associated data.  |
|                           | tagPtr  | Contains the pointer to the Tag to be verified.   |
|                           | tagLength   | Contains the length in bytes of the Tag to be verified.   |
| <b>Parameters (inout)</b> | plaintext LengthPtr   | Holds a pointer to the memory location in which the output length in bytes of the plaintext 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. |
| <b>Parameters (out)</b>   | plaintextPtr  | Contains the pointer to the data where the decrypted data shall be stored.  |
|                           | verifyPtr   | Contains the pointer to the result of the verification.   |

|                      |  |  |
|----------------------|--|--|
| <b>Return value</b>  | Std_Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>   | 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. |  |
| <b>Available via</b> | Csm.h  |  |

l()

### 8.3.6 Signature Interface

A digital signature is a type of asymmetric cryptography. Digital signatures are equivalent to traditional handwritten signatures in many respects. Digital signatures can be used to authenticate the source of messages as well as to prove integrity of signed messages. If a message is digitally signed, any change in the message after signature will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature.

#### 8.3.6.1 Csm\_SignatureGenerate

[SWS\_Csm\_00992]

|                         |   |  |
|-------------------------|---|--|
| <b>Service Name</b>     | Csm_SignatureGenerate   |  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_SignatureGenerate (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* dataPtr,     uint32 dataLength,     uint8* resultPtr,     uint32* resultLengthPtr )</pre> |  |
| <b>Service ID [hex]</b> | 0x76  |  |
| <b>Sync/Async</b>       | Asynchronous or Async, dependend on the job configuration   |  |
| <b>Reentrancy</b>       | Reentrant   |  |
| <b>Parameters (in)</b>  | jobId   | Holds the identifier of the job using the CSM service. |
|                         | mode  | Indicates which operation mode(s) to perform.          |
|                         | dataPtr   | Contains the pointer to the data to be signed.         |



|                           |   |  |
|---------------------------|---|--|
|                           | data Length   | Contains the number of bytes to sign.  |
| <b>Parameters (inout)</b> | result Length Ptr   | 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.  |
| <b>Parameters (out)</b>   | resultPtr   | Contains the pointer to the data where the signature shall be stored.  |
| <b>Return value</b>       | Std - Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Uses the given data to perform the signature calculation and stores the signature in the memory location pointed by the result pointer. |  |
| <b>Available via</b>      | Csm.h   |  |

](SRS\_CryptoStack\_00023)

### 8.3.6.2 Csm\_SignatureVerify

[SWS\_Csm\_00996]

|                         |   |   |
|-------------------------|---|---|
| <b>Service Name</b>     | Csm_SignatureVerify   |   |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_SignatureVerify (     uint32 jobId,     Crypto_OperationModeType mode,     const uint8* dataPtr,     uint32 dataLength,     const uint8* signaturePtr,     uint32 signatureLength,     Crypto_VerifyResultType* verifyPtr )</pre> |   |
| <b>Service ID [hex]</b> | 0x64  |   |
| <b>Sync/Async</b>       | Asynchronous or Async, dependend on the job configuration   |   |
| <b>Reentrancy</b>       | Reentrant   |   |
| <b>Parameters (in)</b>  | jobId   | Holds the identifier of the job using the CSM service.  |
|                         | mode  | The Crypto_JobInfoType job with the corresponding jobId shall be modified in the following way: |
|                         | dataPtr   | Contains the pointer to the data to be verified.  |
|                         | dataLength  | Contains the number of data bytes.  |

|                           |  |  |
|---------------------------|--|--|
|                           | signaturePtr   | Holds a pointer to the signature to be verified.   |
|                           | signature Length   | Contains the signature length in bytes.  |
| <b>Parameters (inout)</b> | None   |  |
| <b>Parameters (out)</b>   | verifyPtr  | Holds a pointer to the memory location, which will hold the result of the signature verification.  |
| <b>Return value</b>       | Std_Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Verifies the given MAC by comparing if the signature is generated with the given data. |  |
| <b>Available via</b>      | Csm.h  |  |

](SRS\_CryptoStack\_00023)

### 8.3.7 Random Interface

The random interface provides generation of random numbers. A random number can be generated either by a physical device (true random number generator), or by computational algorithms (pseudo random number generator). The randomness of pseudo random number generators can be increased by an appropriate selection of the seed.

#### 8.3.7.1 Csm\_RandomGenerate

[SWS\_Csm\_01543]

|                         |  |  |
|-------------------------|--|--|
| <b>Service Name</b>     | Csm_RandomGenerate   |  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_RandomGenerate (     uint32 jobId,     uint8* resultPtr,     uint32* resultLengthPtr )</pre> |  |
| <b>Service ID [hex]</b> | 0x72   |  |
| <b>Sync/Async</b>       | Asynchronous or Async, dependend on the job configuration  |  |
| <b>Reentrancy</b>       | Reentrant  |  |
| <b>Parameters</b>       | jobId  | Holds the identifier of the job using the CSM service. |

|                           |  |   |
|---------------------------|--|---|
| <b>(in)</b>               |  |   |
| <b>Parameters (inout)</b> | result Length Ptr  | 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. |
| <b>Parameters (out)</b>   | resultPtr  | Holds a pointer to the memory location which will hold the result of the random number generation.  |
| <b>Return value</b>       | Std_ - Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_ENTROPY_EXHAUSTED: Request failed, entropy of random number generator is exhausted   |
| <b>Description</b>        | Generate a random number and stores it in the memory location pointed by the result pointer. |   |
| <b>Available via</b>      | Csm.h  |   |

](SRS\_CryptoStack\_00019)

To generate a random number, no streaming approach is necessary. The interface `Csm_RandomGenerate` can be called arbitrarily often to generate multiple random numbers.

**[SWS\_Csm\_01054]** [ The operation mode of the `Csm_RandomGenerate()` function call shall be set to "CRYPTO\_OPERATIONMODE\_SINGLECALL".

]()

### 8.3.8 Key Management Interface

The following interfaces are used for key management. Basically, a key contains of one ore more key elements. A key element can be part of multiple keys. For example, this allows to derive a key element from a password with one keyId, and to use this derived key element for encryption with another keyId.

Note:

If the actual key element to be modified is directly mapped to flash memory, there could be a bigger delay when calling the key management functions (synchronous operation)

**[SWS\_Csm\_00974]** [ If a key management function is called, the CSM shall disable processing new jobs from the queue until the next call of the main function.

]()

#### 8.3.8.1 Key Setting Interface

##### 8.3.8.1.1 Csm\_KeyElementSet [SWS\_Csm\_00957][

|                           |  |  |
|---------------------------|--|--|
| <b>Service Name</b>       | Csm_KeyElementSet  |  |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_KeyElementSet (     uint32 keyId,     uint32 keyElementId,     const uint8* keyPtr,     uint32 keyLength )</pre> |  |
| <b>Service ID [hex]</b>   | 0x78   |  |
| <b>Sync/Async</b>         | Synchronous  |  |
| <b>Reentrancy</b>         | Non Reentrant  |  |
| <b>Parameters (in)</b>    | keyId  | Holds the identifier of the key for which a new material shall be set.   |
|                           | keyElement Id  | Holds the identifier of the key element to be written.   |
|                           | keyPtr   | Holds the pointer to the key element bytes to be processed.  |
|                           | keyLength  | Contains the number of key element bytes.  |
| <b>Parameters (inout)</b> | None   |  |
| <b>Parameters (out)</b>   | None   |  |
| <b>Return value</b>       | Std_Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_WRITE_FAIL: Request failed because write access was denied<br>CRYPTO_E_KEY_NOT_AVAILABLE: Request failed because the key is not available<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element size does not match size of provided data |
| <b>Description</b>        | Sets the given key element bytes to the key identified by keyId.   |  |
| <b>Available via</b>      | Csm.h  |  |

]()

**[SWS\_Csm\_01002]** | If no errors are detected by Csm, the service

Csm\_KeyElementSet() shall call CryIf\_KeyElementSet().

]()

### 8.3.8.1.2 Csm\_KeySetValid

**[SWS\_Csm\_00958]**

|                     |  |  |
|---------------------|--|--|
| <b>Service Name</b> | Csm_KeySetValid  |  |
| <b>Syntax</b>       | <pre>Std_ReturnType Csm_KeySetValid (     uint32 keyId )</pre> |  |

|                           |   |   |
|---------------------------|---|---|
| <b>Service ID [hex]</b>   | 0x67  |   |
| <b>Sync/Async</b>         | Synchronous   |   |
| <b>Reentrancy</b>         | Non Reentrant   |   |
| <b>Parameters (in)</b>    | keyId   | Holds the identifier of the key for which a new material shall be validated.  |
| <b>Parameters (inout)</b> | None  |   |
| <b>Parameters (out)</b>   | None  |   |
| <b>Return value</b>       | Std_Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy |
| <b>Description</b>        | Sets the key state of the key identified by keyId to valid. |   |
| <b>Available via</b>      | Csm.h   |   |

}]()

**[SWS\_Csm\_01003]** | If no errors are detected by Csm, the service Csm\_KeySetValid() shall call CryIf\_KeySetValid().

}]()

### 8.3.8.2 Key Extraction Interface

#### 8.3.8.2.1 Csm\_KeyElementGet

**[SWS\_Csm\_00959]**

|                         |  |  |
|-------------------------|--|--|
| <b>Service Name</b>     | Csm_KeyElementGet  |  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_KeyElementGet (     uint32 keyId,     uint32 keyElementId,     uint8* keyPtr,     uint32* keyLengthPtr )</pre> |  |
| <b>Service ID [hex]</b> | 0x68   |  |
| <b>Sync/Async</b>       | Synchronous  |  |
| <b>Reentrancy</b>       | Reentrant  |  |
| <b>Parameters (in)</b>  | keyId  | Holds the identifier of the key from which a key element shall be extracted. |
|                         | keyElementId   | Holds the identifier of the key element to be extracted.                     |
| <b>Parameters</b>       | key  | Holds a pointer to the memory location in which the output buffer length     |

|                         |  |  |
|-------------------------|--|--|
| <b>(inout)</b>          | LengthPtr  | in bytes is stored. On calling this function, this parameter shall contain the buffer length in bytes of the keyPtr. When the request has finished, the actual size of the written input bytes shall be stored.  |
| <b>Parameters (out)</b> | keyPtr   | Holds the pointer to the memory location where the key shall be copied to.   |
| <b>Return value</b>     | Std_ReturnType   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_NOT_AVAILABLE: Request failed, the requested key element is not available<br>CRYPTO_E_KEY_READ_FAIL: Request failed because read access was denied<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>      | 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. |  |
| <b>Available via</b>    | Csm.h  |  |

|(SRS\_CryptoStack\_00010, SRS\_CryptoStack\_00011, SRS\_CryptoStack\_00029)

**[SWS\_Csm\_01004]** | If no errors are detected by Csm, the service

Csm\_KeyElementGet () shall call CryIf\_KeyElementGet ().

| ( )

The underlying Crypto Driver has to decide if and how the key element bytes are extracted.

### 8.3.8.3 Key Copying Interface

#### 8.3.8.3.1 Csm\_KeyElementCopy

**[SWS\_Csm\_00969]**|

|                         |   |  |
|-------------------------|---|--|
| <b>Service Name</b>     | Csm_KeyElementCopy  |  |
| <b>Syntax</b>           | Std_ReturnType Csm_KeyElementCopy (<br>const uint32 keyId,<br>const uint32 keyElementId,<br>const uint32 targetKeyId,<br>const uint32 targetKeyElementId<br>) |  |
| <b>Service ID [hex]</b> | 0x71  |  |
| <b>Sync/Async</b>       | Synchronous   |  |
| <b>Reentrancy</b>       | Reentrant, but not for the same keyId   |  |
| <b>Parameters (in)</b>  | keyId   | Holds the identifier of the key whose key element shall be the source element. |
|                         | keyElementId  | Holds the identifier of the key element which shall be the source              |

|                           |   |  |
|---------------------------|---|--|
|                           |   | for the copy operation.  |
|                           | targetKeyId   | Holds the identifier of the key whose key element shall be the destination element.  |
|                           | targetKeyElementId  | Holds the identifier of the key element which shall be the destination for the copy operation.   |
| <b>Parameters (inout)</b> | None  |  |
| <b>Parameters (out)</b>   | None  |  |
| <b>Return value</b>       | Std_Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_NOT_AVAILABLE: Request failed, the requested key element is not available<br>CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element<br>CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | This function shall copy a key elements from one key to a target key. |  |
| <b>Available via</b>      | Csm.h   |  |

}|()

**[SWS\_Csm\_01032]** | If no errors are detected by Csm and the `keyId` and `targetKeyId` are located in different Crypto Drivers, the service `Csm_KeyElementCopy()` shall call `CryIf_KeyElementCopy()` and pass on the return value.

}|()

### 8.3.8.3.2 Csm\_KeyCopy

**[SWS\_Csm\_01034]** |

|                         |  |
|-------------------------|--|
| <b>Service Name</b>     | Csm_KeyCopy  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_KeyCopy (     const uint32 keyId,     const uint32 targetKeyId )</pre> |
| <b>Service ID [hex]</b> | 0x73   |
| <b>Sync/Async</b>       | Synchronous  |
| <b>Reentrancy</b>       | Reentrant, but not for same keyId  |

|                           |  |  |
|---------------------------|--|--|
| <b>Parameters (in)</b>    | keyId  | Holds the identifier of the key whose key element shall be the source element.   |
|                           | targetKeyId  | Holds the identifier of the key whose key element shall be the destination element.  |
| <b>Parameters (inout)</b> | None   |  |
| <b>Parameters (out)</b>   | None   |  |
| <b>Return value</b>       | Std_Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_NOT_AVAILABLE: Request failed, the requested key element is not available<br>CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element<br>CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | This function shall copy all key elements from the source key to a target key. |  |
| <b>Available via</b>      | Csm.h  |  |

|()

**[SWS\_Csm\_01035]** | 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_KeyCopy()` and pass on the return value.

|()

### 8.3.8.3.3 Csm\_KeyElementCopyPartial

**[SWS\_Csm\_91025]**|

|                         |   |
|-------------------------|---|
| <b>Service Name</b>     | Csm_KeyElementCopyPartial   |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_KeyElementCopyPartial (     uint32 keyId,     uint32 keyElementId,     uint32 keyElementSourceOffset,     uint32 keyElementTargetOffset,     uint32 keyElementCopyLength,     uint32 targetKeyId,     uint32 targetKeyElementId )</pre> |
| <b>Service ID [hex]</b> | 0x79  |
| <b>Sync/Async</b>       | Synchronous   |



|                           |   |  |
|---------------------------|---|--|
| <b>Reentrancy</b>         | Reentrant, but not for the same keyId   |  |
| <b>Parameters (in)</b>    | keyId   | Holds the identifier of the key whose key element shall be the source element for copy operation.  |
|                           | keyElementId  | Holds the identifier of the key element which shall be the source for the copy operation.  |
|                           | keyElementSourceOffset  | This is the offset of the source key element indicating the start index of the copy operation.   |
|                           | keyElementTargetOffset  | This is the offset of the destination key element indicating the start index of the copy operation.  |
|                           | keyElementCopyLength  | Specifies the number of bytes that shall be copied.  |
|                           | targetKeyId   | Holds the identifier of the key whose key element shall be the destination element.  |
|                           | targetKeyElementId  | Holds the identifier of the key element which shall be the destination for the copy operation.   |
| <b>Parameters (inout)</b> | None  |  |
| <b>Parameters (out)</b>   | None  |  |
| <b>Return value</b>       | Std_ReturnType  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_NOT_AVAILABLE: Request failed, the requested key element is not available<br>CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element<br>CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Copies a key element to another key element in the same crypto driver. The key ElementSourceOffset and keyElementCopyLength allows to copy just a part of the source key element into the destination. The offset into the target key is also specified with this function. |  |
| <b>Available via</b>      | Csm.h   |  |

l()

**Note:** A Concatenation of partial keys into one key element is possible by calling Csm\_KeyElementCopyPartial() multiple times and adjusting keyElementTargetOffset properly.

**[SWS\_Csm\_91019]** | If no errors are detected by Csm shall call `CryIf_KeyElementCopyPartial()` and pass on the return value.  
|()

**[SWS\_Csm\_91020]** | If the current length of the target key element is greater or equal than  $(keyElementTargetOffset + keyElementCopyLength)$ , the key element length remains unchanged and the target data is overwritten with the contents of the source data.  
|()

**[SWS\_Csm\_91021]** | If the current length of the target key element is lower than  $(keyElementTargetOffset + keyElementCopyLength)$  and the maximum length of the key element is greater or equal than  $(keyElementTargetOffset + keyElementCopyLength)$ , then the source data shall be copied into the target key element and the length shall be set to  $(keyElementTargetOffset + keyElementCopyLength)$ .  
|()

**[SWS\_Csm\_91022]** |  
If the maximum length of the target key element is lower than  $(keyElementTargetOffset + keyElementCopyLength)$  then the copy operation shall not be performed and the function shall return with the error code `CRYPTO_E_KEY_SIZE_MISMATCH`.  
|()

#### 8.3.8.4 Key Generation interface

The key generation interface is used to generate a key into the key element `CRYPTO_KE_KEYGENERATE_KEY` according to the algorithm defined in the key element `CRYPTO_KE_KEYGENERATE_ALGORITHM`.

The key will be generated from the random value that is located in the key element `CRYPTO_KE_KEYGENERATE_SEED`.

The random value can be generated, for example, with the function `Csm_RandomGenerate()` and must be stored in `CRYPTO_KE_KEYGENERATE_SEED` before the key generation is triggered.

It is important to check the quality of the randomness and its entropy of the seed, which depends on the used hardware, and software of a stack. The randomness has a major impact on the quality of the generated key material.

The key element with the `id=CRYPTO_KE_KEYGENERATE_ALGORITHM` contains a type from "Crypto\_AlgorithmFamilyType", e.g. `CRYPTO_ALGOFAM_AES`, `CRYPTO_ALGOFAM_RSA` or `CRYPTO_ALGOFAM_ED25519`, that allows to generate an adequate key.

As a counter example, the algorithm family type `CRYPTO_ALGOFAM_SHA2_256` is not adequate because it provides no hint what key shall be generated.

For the key element `CRYPTO_KE_KEYGENERATE_KEY` the key element configuration item `CryptoKeyElement/CryptoKeyElementFormat` indicates the format of the generated key.

### 8.3.8.4.1 Csm\_RandomSeed

[SWS\_Csm\_01051]

|                           |  |   |
|---------------------------|--|---|
| <b>Service Name</b>       | Csm_RandomSeed   |   |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_RandomSeed (     uint32 keyId,     const uint8* seedPtr,     uint32 seedLength )</pre> |   |
| <b>Service ID [hex]</b>   | 0x69   |   |
| <b>Sync/Async</b>         | Synchronous  |   |
| <b>Reentrancy</b>         | Reentrant, but not for same keyId  |   |
| <b>Parameters (in)</b>    | keyId  | Holds the identifier of the key for which a new seed shall be generated.  |
|                           | seedPtr  | Holds a pointer to the memory location which contains the data to feed the seed.  |
|                           | seedLength   | Contains the length of the seed in bytes.   |
| <b>Parameters (inout)</b> | None   |   |
| <b>Parameters (out)</b>   | None   |   |
| <b>Return value</b>       | Std_Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid" |
| <b>Description</b>        | Feeds the key element CRYPTO_KE_RANDOM_SEED with a random seed.  |   |
| <b>Available via</b>      | Csm.h  |   |

]()

[SWS\_Csm\_01052] [ If no errors are detected by Csm, the service Csm\_RandomSeed() shall call CryIf\_RandomSeed(). ]()

### 8.3.8.4.2 Csm\_KeyGenerate

[SWS\_Csm\_00955]

|                         |  |  |
|-------------------------|--|--|
| <b>Service Name</b>     | Csm_KeyGenerate  |  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_KeyGenerate (     uint32 keyId )</pre> |  |
| <b>Service ID [hex]</b> | 0x6a   |  |

|                           |   |   |
|---------------------------|---|---|
| <b>Sync/Async</b>         | Synchronous   |   |
| <b>Reentrancy</b>         | Reentrant but not for same keyId  |   |
| <b>Parameters (in)</b>    | keyId   | Holds the identifier of the key for which a new material shall be generated.  |
| <b>Parameters (inout)</b> | None  |   |
| <b>Parameters (out)</b>   | None  |   |
| <b>Return value</b>       | Std_Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Generates new key material and store it in the key identified by keyId. |   |
| <b>Available via</b>      | Csm.h   |   |

](SRS\_CryptoStack\_00026, SRS\_CryptoStack\_00027)

**[SWS\_Csm\_01005]** [ If no errors are detected by Csm, the service `Csm_KeyGenerate()` shall call `CryIf_KeyGenerate()`.  
]()

### 8.3.8.5 Key Derivation Interface

In cryptography, a key derivation function (or KDF) is a function, which derives one or more secret keys from a secret value and/or other known information such as a passphrase or cryptographic key.

Specification of input keys that are protected by hardware means can be achieved by using the `Csm_KeyDeriveKey` interface.

#### 8.3.8.5.1 Csm\_KeyDerive

**[SWS\_Csm\_00956]**

|                         |  |
|-------------------------|--|
| <b>Service Name</b>     | Csm_KeyDerive  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_KeyDerive (     uint32 keyId,     uint32 targetKeyId )</pre> |
| <b>Service ID [hex]</b> | 0x6b   |
| <b>Sync/Async</b>       | Synchronous  |
| <b>Reentrancy</b>       | Reentrant, but not for same keyId  |

|                           |   |   |
|---------------------------|---|---|
| <b>Parameters (in)</b>    | keyId   | Holds the identifier of the key which is used for key derivation.   |
|                           | targetKeyId   | Holds the identifier of the key which is used to store the derived key.   |
| <b>Parameters (inout)</b> | None  |   |
| <b>Parameters (out)</b>   | None  |   |
| <b>Return value</b>       | Std_Return-Type   | <p>E_OK: Request successful<br/> E_NOT_OK: Request failed<br/> CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br/> CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element<br/> CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element<br/> CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br/> CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible<br/> CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element</p> |
| <b>Description</b>        | Derives a new key by using the key elements in the given key identified by the keyId. The given key contains the key elements for the password and salt. The derived key is stored in the key element with the id 1 of the key identified by targetCryptoKeyId. |   |
| <b>Available via</b>      | Csm.h   |   |

### |(SRS\_CryptoStack\_00103)Csm\_KeyGenerate

**[SWS\_Csm\_01018]** | If no errors are detected by Csm, the service Csm\_KeyDerive () shall call CryIf\_KeyDerive ().  
|()

**[SWS\_Csm\_01019]** | If the number of iterations for the key derivation is needed by the Crypto Driver, it shall be stored in the key element CRYPTO\_KE\_KEYDERIVATION\_ITERATIONS.  
|()

#### 8.3.8.6 Key Exchange Interface

Two users that each have a private secret can use a key exchange protocol to obtain a common secret, e.g. a key for a symmetric-key algorithm, without telling each other their private secret and without any listener being able to obtain the common secret or their private secrets

The functions Csm\_KeyExchangeCalcPubVal () / Csm\_JobKeyExchangeCalcPubVal () and Csm\_KeyExchangeCalcSecret () / Csm\_JobKeyExchangeCalcSecret () are used to support Diffie-Hellman (DH) key exchange.

This allows two partners, Alice and Bob, to generate private and public key material, to exchange public parts so that both parties can generate at the end a common shared secret. This shared secret can further be used, e.g. for symmetric data operation such as data encryption or MAC generation.

The public and private key material can either be based on prime based large number as it is used with RSA or on elliptic curve (so-called elliptic-curve diffie-hellman).

The CSM key exchange functions require a key with key elements according to [SWS\_Csm\_01022], in the line of Crypto Service "Key Exchange". The key elements `CRYPTO_KE_KEYEXCHANGE_BASE`, `CRYPTO_KE_KEYEXCHANGE_PRIVKEY` and `CRYPTO_KE_KEYEXCHANGE_OWNPUKEY` are used to hold the public/private key material.

These values can either be pre-defined and set by `Csm_KeyElementSet()` followed by `Csm_KeySetValid()` or generated. For example, these key values can be generated by `Csm_KeyGenerate()` and then copied with `Csm_KeyElementCopy()` to the corresponding key elements, followed by a call to `Csm_KeySetValid()`.

In a first step, Alice will call `Csm_KeyExchangeCalcPubVal()` / `Csm_JobKeyExchangeCalcPubVal()` and send the results to Bob (exchanged data may need to be signed and/or encrypted depending on the protocol).

It should be noted, that if `KeyExchangeCalcPubVal` is called but no valid key material exists (key is not valid or essential key elements have length=0), the function shall generate the necessary key material and continue as normal.

If needed, Bob will put received key material from Alice into the corresponding key elements. He will also call `Csm_KeyExchangeCalcPubVal()` to generate his shared value that needs to be sent to Alice. Afterwards, Bob can call `Csm_KeyExchangeCalcSecret()` to generate the common secret. This value will be placed into the key element `CYRPTO_KE_KEYEXCHANGE_SHAREDVALUE`.

When Alice receives the public value from Bob, it will call `KeyExchangeCalcSecret()` and provides the value from Bob in the parameter of the function. The common shared secret will be generated by this function into the key element `CYRPTO_KE_KEYEXCHANGE_SHAREDVALUE`.

Depending on the algorithm, Bob needs to send key material to Alice to allow her to generate the common shared secret.

The key element `CRYPTO_KE_KEYEXCHANGE_ALGORITHM` specifies the Diffie-Hellman algorithm. The key element value is of type `Crypto_AlgorithmFamily`, for example `CRYPTO_ALGOFAM_DH` (for modulo based DH) or `CRYPTO_ALGOFAM_ED25519` (for ECDH(E)).

Additional elliptic curve parameter can be specified with the additional key element `CRYPTO_KE_KEYEXCHANGE_CURVE`.

The other key elements have the following meaning:

|   | DH(E)          | ECDH(E)         |
|---|----------------|-----------------|
| <code>CRYPTO_KE_KEYEXCHANGE_BASE</code>     | Modulo         | Generator point |
| <code>CRYPTO_KE_KEYEXCHANGE_PRIVKEY</code>  | Local exponent | Private key     |
| <code>CRYPTO_KE_KEYEXCHANGE_OWNPUKEY</code> | Generator      | Public key      |

**8.3.8.6.1 Csm\_KeyExchangeCalcPubVal**  
**[SWS\_Csm\_00966]**

|                           |  |  |
|---------------------------|--|--|
| <b>Service Name</b>       | Csm_KeyExchangeCalcPubVal  |  |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_KeyExchangeCalcPubVal (     uint32 keyId,     uint8* publicValuePtr,     uint32* publicValueLengthPtr )</pre>                      |  |
| <b>Service ID [hex]</b>   | 0x6c   |  |
| <b>Sync/Async</b>         | Synchronous  |  |
| <b>Reentrancy</b>         | Reentrant but not for same keyId   |  |
| <b>Parameters (in)</b>    | keyId  | Holds the identifier of the key which shall be used for the key exchange protocol.   |
| <b>Parameters (inout)</b> | public Value LengthPtr   | 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. |
| <b>Parameters (out)</b>   | public ValuePtr  | Contains the pointer to the data where the public value shall be stored.   |
| <b>Return value</b>       | Std_Return-Type  | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element                    |
| <b>Description</b>        | 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. |  |
| <b>Available via</b>      | Csm.h  |  |

](SRS\_CryptoStack\_00028)

**[SWS\_Csm\_01020]** [ If no errors are detected by Csm, the service Csm\_KeyExchangeCalcPubVal() shall call CryIf\_KeyExchangeCalcPubVal(). ]()

**8.3.8.6.2 Csm\_KeyExchangeCalcSecret**  
**[SWS\_Csm\_00967]**

|                     |                           |
|---------------------|---------------------------|
| <b>Service Name</b> | Csm_KeyExchangeCalcSecret |
|---------------------|---------------------------|



|                           |  |   |
|---------------------------|--|---|
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_KeyExchangeCalcSecret (     uint32 keyId,     const uint8* partnerPublicValuePtr,     uint32 partnerPublicValueLength )</pre>  |   |
| <b>Service ID [hex]</b>   | 0x6d   |   |
| <b>Sync/Async</b>         | Synchronous  |   |
| <b>Reentrancy</b>         | Reentrant but not for same keyId   |   |
| <b>Parameters (in)</b>    | keyId  | Holds the identifier of the key which shall be used for the key exchange protocol.  |
|                           | partnerPublicValuePtr  | Holds the pointer to the memory location which contains the partner's public value.   |
|                           | partnerPublicValueLength   | Contains the length of the partner's public value in bytes.   |
| <b>Parameters (inout)</b> | None   |   |
| <b>Parameters (out)</b>   | None   |   |
| <b>Return value</b>       | Std_ReturnType   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Calculates the shared secret key for the key exchange with the key material of the key identified by the keyId and the partner public key. The shared secret key is stored as a key element in the same key. |   |
| <b>Available via</b>      | Csm.h  |   |

](SRS\_CryptoStack\_00028)

**[SWS\_Csm\_01006]** [ If no errors are detected by Csm, the service Csm\_KeyExchangeCalcSecret () shall call CryIf\_KeyExchangeCalcSecret (). ] ( )

### 8.3.9 Cryptographic Primitives and Schemes

The keyId configured in the Job is only used to determine which driver objects needs to be used for the specific JobKeyPrimitive operation.



### 8.3.9.1 Csm\_JobKeySetValid

#### [SWS\_Csm\_91027]

|                           |   |   |
|---------------------------|---|---|
| <b>Service Name</b>       | Csm_JobKeySetValid  |   |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_JobKeySetValid (     uint32 jobId,     uint32 keyId )</pre>         |   |
| <b>Service ID [hex]</b>   | 0x7a  |   |
| <b>Sync/Async</b>         | Sync or Async, depending on the job configuration   |   |
| <b>Reentrancy</b>         | Reentrant   |   |
| <b>Parameters (in)</b>    | jobId   | Holds the identifier of the job using the CSM service.  |
|                           | keyId   | Holds the identifier of the key for which a new material shall be validated.  |
| <b>Parameters (inout)</b> | None  |   |
| <b>Parameters (out)</b>   | None  |   |
| <b>Return value</b>       | Std_Return-<br>Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, Crypro Driver Object is busy |
| <b>Description</b>        | Stores the key if necessary and sets the key state of the key identified by keyId to valid. |   |
| <b>Available via</b>      | Csm.h   |   |

()

### 8.3.9.2 Csm\_JobRandomSeed

#### [SWS\_Csm\_91028]

|                         |   |  |
|-------------------------|---|--|
| <b>Service Name</b>     | Csm_JobRandomSeed   |  |
| <b>Syntax</b>           | <pre>Std_ReturnType Csm_JobRandomSeed (     uint32 jobId,     uint32 keyId,     const uint8* seedPtr,     uint32 seedLength )</pre> |  |
| <b>Service ID [hex]</b> | 0x7b  |  |
| <b>Sync/Async</b>       | Asynchronous or Async, depending on the job configuration   |  |
| <b>Reentrancy</b>       | Reentrant   |  |
| <b>Parameters (in)</b>  | jobId   | Holds the identifier of the job using the CSM service. |

|                           |   |  |
|---------------------------|---|--|
|                           | keyId   | Holds the identifier of the key for which a new seed shall be generated.   |
|                           | seedPtr   | Holds a pointer to the memory location which contains the data to feed the seed.   |
|                           | seedLength  | Contains the length of the seed in bytes.  |
| <b>Parameters (inout)</b> | None  |  |
| <b>Parameters (out)</b>   | None  |  |
| <b>Return value</b>       | Std_Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid" |
| <b>Description</b>        | This function shall dispatch the random seed function to the configured crypto driver object. |  |
| <b>Available via</b>      | Csm.h   |  |

]()

Note: The provided key Id(s) shall be transformed from CsmKeyId's to CryIfKeyId's.

### 8.3.9.3 Csm\_JobKeyGenerate

[SWS\_Csm\_91029]

|                           |   |  |
|---------------------------|---|--|
| <b>Service Name</b>       | Csm_JobKeyGenerate  |  |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_JobKeyGenerate (     uint32 jobId,     uint32 keyId )</pre> |  |
| <b>Service ID [hex]</b>   | 0x7c  |  |
| <b>Sync/Async</b>         | Asynchronous or Async, depending on the job configuration                           |  |
| <b>Reentrancy</b>         | Reentrant   |  |
| <b>Parameters (in)</b>    | jobId   | Holds the identifier of the job using the CSM service.   |
|                           | keyId   | Holds the identifier of the key for which a new material shall be generated.                                 |
| <b>Parameters (inout)</b> | None  |  |
| <b>Parameters (out)</b>   | None  |  |
| <b>Return value</b>       | Std_Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy |

|                      |  |  |
|----------------------|--|--|
|                      |  | CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>   | Generates new key material and stores it in the key identified by keyId. |  |
| <b>Available via</b> | Csm.h  |  |

]()

Note: The provided key Id(s) shall be transformed from CsmKeyId's to CrylIfKeyId's.

### 8.3.9.4 Csm\_JobKeyDerive

[SWS\_Csm\_91030]

|                           |   |  |
|---------------------------|---|--|
| <b>Service Name</b>       | Csm_JobKeyDerive  |  |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_JobKeyDerive (     uint32 jobId,     uint32 keyId,     uint32 targetKeyId )</pre> |  |
| <b>Service ID [hex]</b>   | 0x7d  |  |
| <b>Sync/Async</b>         | Asynchronous or Async, depending on the job configuration   |  |
| <b>Reentrancy</b>         | Reentrant   |  |
| <b>Parameters (in)</b>    | jobId   | Holds the identifier of the job using the CSM service.   |
|                           | keyId   | Holds the identifier of the key which is used for key derivation.  |
|                           | targetKeyId   | Holds the identifier of the key which is used to store the derived key.  |
| <b>Parameters (inout)</b> | None  |  |
| <b>Parameters (out)</b>   | None  |  |
| <b>Return value</b>       | Std_Return-Type   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element<br>CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible<br>CRYPTO_E_KEY_EMPTY: Request failed because of |

|                      |   |
|----------------------|---|
|                      | uninitialized source key element  |
| <b>Description</b>   | Derives a new key by using the key elements in the given key identified by the keyId. The given key contains the key elements for the password and salt. The derived key is stored in the key element with the id 1 of the key identified by targetCryptoKeyId. |
| <b>Available via</b> | Csm.h   |

]()

Note: The provided key Id(s) shall be transformed from CsmKeyId's to CryIfKeyId's.

### 8.3.9.5 Csm\_JobKeyExchangeCalcPubVal

[SWS\_Csm\_91031]

|                           |  |  |
|---------------------------|--|--|
| <b>Service Name</b>       | Csm_JobKeyExchangeCalcPubVal   |  |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_JobKeyExchangeCalcPubVal (     uint32 jobId,     uint32 keyId,     uint8* publicValuePtr,     uint32* publicValueLengthPtr )</pre> |  |
| <b>Service ID [hex]</b>   | 0x7e   |  |
| <b>Sync/Async</b>         | Asynchronous or Async, depending on the job configuration  |  |
| <b>Reentrancy</b>         | Reentrant  |  |
| <b>Parameters (in)</b>    | jobId  | Holds the identifier of the job using the CSM service.   |
|                           | keyId  | Holds the identifier of the key which shall be used for the key exchange protocol.   |
| <b>Parameters (inout)</b> | public Value LengthPtr   | 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. |
| <b>Parameters (out)</b>   | public ValuePtr  | Contains the pointer to the data where the public value shall be stored.   |
| <b>Return value</b>       | Std_ReturnType   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element                           |
| <b>Description</b>        | 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. |  |

|                      |       |
|----------------------|-------|
| <b>Available via</b> | Csm.h |
|----------------------|-------|

J()

Note: The provided key Id(s) shall be transformed from CsmKeyId's to CrylfKeyId's.

### 8.3.9.6 Csm\_JobKeyExchangeCalcSecret

#### [SWS\_Csm\_91032]

|                           |  |  |
|---------------------------|--|--|
| <b>Service Name</b>       | Csm_JobKeyExchangeCalcSecret   |  |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_JobKeyExchangeCalcSecret (     uint32 jobId,     uint32 keyId,     const uint8* partnerPublicValuePtr,     uint32 partnerPublicValueLength )</pre>                                   |  |
| <b>Service ID [hex]</b>   | 0x7f   |  |
| <b>Sync/Async</b>         | Asynchronous or Async, depending on the job configuration  |  |
| <b>Reentrancy</b>         | Reentrant  |  |
| <b>Parameters (in)</b>    | jobId  | Holds the identifier of the job using the CSM service.   |
|                           | keyId  | Holds the identifier of the key which shall be used for the key exchange protocol.   |
|                           | partnerPublicValuePtr  | Holds the pointer to the memory location which contains the partner's public value.  |
|                           | partnerPublicValue Length  | Contains the length of the partner's public value in bytes.  |
| <b>Parameters (inout)</b> | None   |  |
| <b>Parameters (out)</b>   | None   |  |
| <b>Return value</b>       | Std_ReturnType   | E_OK: Request successful<br>E_NOT_OK: Request failed<br>CRYPTO_E_BUSY: Request failed, service is still busy<br>CRYPTO_E_KEY_NOT_VALID: Request failed, the key's state is "invalid"<br>CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element |
| <b>Description</b>        | Calculates the shared secret key for the key exchange with the key material of the key identified by the keyId and the partner public key. The shared secret key is stored as a key element in the same key. |  |
| <b>Available via</b>      | Csm.h  |  |

]()

Note: The provided key Id(s) shall be transformed from CsmKeyId's to CrylfKeyId's.

### 8.3.10 Job Cancellation Interface

#### 8.3.10.1 Csm\_CancelJob

[SWS\_Csm\_00968]

|                           |   |   |
|---------------------------|---|---|
| <b>Service Name</b>       | Csm_CancelJob   |   |
| <b>Syntax</b>             | <pre>Std_ReturnType Csm_CancelJob (     uint32 job,     Crypto_OperationModeType mode )</pre> |   |
| <b>Service ID [hex]</b>   | 0x6f  |   |
| <b>Sync/Async</b>         | Synchronous   |   |
| <b>Reentrancy</b>         | Non Reentrant   |   |
| <b>Parameters (in)</b>    | job   | Holds the identifier of the job to be canceled  |
|                           | mode  | Not used, just for interface compatibility provided.  |
| <b>Parameters (inout)</b> | None  |   |
| <b>Parameters (out)</b>   | None  |   |
| <b>Return value</b>       | Std_ReturnType  | E_OK: Request successful. Job removed from any queue and potentially from crypto driver hardware.<br>E_NOT_OK: Request failed<br>CRYPTO_E_JOB_CANCELED: Immediate cancelation not possible. The cancelation will be done at next suitable processing step and notified via a negative job's closing callback. |
| <b>Description</b>        | Cancels the job processing from asynchronous or streaming jobs.                               |   |
| <b>Available via</b>      | Csm.h   |   |

]()

[SWS\_Csm\_01086] | If development error detection for the CSM is enabled: The function `Csm_CancelJob()` shall raise the error `CSM_E_PROCESSING_MODE` and return `E_NOT_OK` if the `Csm_CancelJob()` is called for a synchronous job.

]()

**[SWS\_Csm\_01021]** [ The Csm shall remove the job from its own queue or call `Crylf_CancelJob()` to cancel a potential job in the driver.] ( )

**[SWS\_Csm\_01030]** [ In case the `CryIf_CancelJob()` returns `E_OK`, the job's closing callback `CallbackNotification` shall be called with a result value of `CRYPTO_E_JOB_CANCELED`. ] ( )

**[SWS\_Csm\_01087]** [In case the `CryIf_CancelJob()` returns `CRYPTO_E_JOB_CANCELED` (i.e. the job was not instantly canceled) the CSM shall postpone the call of the job's closing callback until the next call of `Csm_CallbackNotification()`. The result of the job's closing callback shall be `CRYPTO_E_JOB_CANCELED`. ] ( )

Note: In case the crypto driver does not support an instant cancelation of the job, the application need to wait for the job's closing callback to free the buffers. The crypto driver could potentially still write to the output buffer(s).

### 8.3.11 Callback Notifications

#### 8.3.11.1 Csm\_CallbackNotification

**[SWS\_Csm\_00970]**

|                           |   |   |
|---------------------------|---|---|
| <b>Service Name</b>       | Csm_CallbackNotification  |   |
| <b>Syntax</b>             | <pre>void Csm_CallbackNotification (     Crypto_JobType* job,     Crypto_ResultType result )</pre>  |   |
| <b>Service ID [hex]</b>   | 0x70  |   |
| <b>Sync/Async</b>         | Synchronous   |   |
| <b>Reentrancy</b>         | Reentrant   |   |
| <b>Parameters (in)</b>    | job   | Holds a pointer to the job, which has finished.     |
|                           | result  | Contains the result of the cryptographic operation. |
| <b>Parameters (inout)</b> | None  |   |
| <b>Parameters (out)</b>   | None  |   |
| <b>Return value</b>       | None  |   |
| <b>Description</b>        | Notifies the CSM that a job has finished. This function is used by the underlying layer (CRYIF). The function name itself is derived from "{CsmJob/CsmJobPrimitive CallbackRef}/CsmCallbackFunc". |   |

|                      |       |
|----------------------|-------|
| <b>Available via</b> | Csm.h |
|----------------------|-------|

|(SRS\_BSW\_00359, SRS\_BSW\_00360)

**[SWS\_Csm\_01044]** If the `CRYPTO_OPERATIONMODE_FINISH` bit is set in `job->jobPrimitiveInputOutput.mode`, the `Csm_CallbackNotification` shall call the configured callback function.

|()

**[SWS\_Csm\_91017]** If the `CRYPTO_OPERATIONMODE_FINISH` bit is set in `job->jobPrimitiveInputOutput.mode` and `CsmProcessingMode` is set to `CRYPTO_PROCESSING_ASYNC` and `CsmJobInterfaceUsePort` is set to `CRYPTO_USE_PORT_OPTIMIZED`, the CSM shall trigger `CallbackNotification` service.

|()

### 8.3.12 Scheduled functions

#### 8.3.12.1 Csm\_MainFunction

**[SWS\_Csm\_00479]**

|                         |   |
|-------------------------|---|
| <b>Service Name</b>     | Csm_MainFunction  |
| <b>Syntax</b>           | void Csm_MainFunction (<br>void<br>)  |
| <b>Service ID [hex]</b> | 0x01  |
| <b>Description</b>      | API to be called cyclically to process the requested jobs. The <code>Csm_MainFunction</code> shall check the queues for jobs to pass to the underlying CRYIF. |
| <b>Available via</b>    | SchM_Csm.h  |

|(SRS\_BSW\_00373, SRS\_BSW\_00432)

## 8.4 Expected Interfaces

### 8.4.1 Interfaces to Standard Software Modules

#### 8.4.2 Mandatory Interfaces

**[SWS\_Csm\_91100]**

| API Function | Header | Description |
|--------------|--------|-------------|
|--------------|--------|-------------|



|                               | <i>File</i> |   |
|-------------------------------|-------------|---|
| Crylf_CancelJob               | Crylf.h     | This interface dispatches the job cancellation function to the configured crypto driver object.   |
| Crylf_KeyCopy                 | Crylf.h     | This function shall copy all key elements from the source key to a target key.  |
| Crylf_Key-ElementCopy         | Crylf.h     | This function shall copy a key elements from one key to a target key.   |
| Crylf_Key-ElementCopy-Partial | Crylf.h     | Copies a key element to another key element. The keyElementOffsets and keyElementCopyLength allows to copy just parts of the source key element into the destination key element. |
| Crylf_Key-ElementGet          | Crylf.h     | This function shall dispatch the get key element function to the configured crypto driver object.   |
| Crylf_Key-ElementSet          | Crylf.h     | This function shall dispatch the set key element function to the configured crypto driver object.   |
| Crylf_Key-ExchangeCalc-Secret | Crylf.h     | This function shall dispatch the key exchange common shared secret calculation function to the configured crypto driver object.   |
| Crylf_Key-Generate            | Crylf.h     | This function shall dispatch the key generate function to the configured crypto driver object.  |
| Crylf_KeySet-Valid            | Crylf.h     | This function shall dispatch the set key valid function to the configured crypto driver object.   |
| Crylf_Process-Job             | Crylf.h     | This interface dispatches the received jobs to the configured crypto driver object.   |
| Crylf_Random-Seed             | Crylf.h     | This function shall dispatch the random seed function to the configured crypto driver object.   |
| Det_Report-RuntimeError       | Det.h       | Service to report runtime errors. If a callout has been configured then this callout shall be called.   |

]()

### 8.4.3 Optional Interfaces

[SWS\_Csm\_91101]

| <i>API Function</i> | <i>Header File</i> | <i>Description</i>                    |
|---------------------|--------------------|---------------------------------------|
| Det_ReportError     | Det.h              | Service to report development errors. |

]()

## 8.4.4 Configurable interfaces

### 8.4.4.1 <Csm\_ApplicationCallbackNotification>

[SWS\_Csm\_00971]

|                           |   |   |
|---------------------------|---|---|
| <b>Service Name</b>       | <Csm_ApplicationCallbackNotification>   |   |
| <b>Syntax</b>             | <pre>void &lt;Csm_ApplicationCallbackNotification&gt; (     const Crypto_JobType* job,     Crypto_ResultType result )</pre>   |   |
| <b>Service ID [hex]</b>   | 0x82  |   |
| <b>Sync/Async</b>         | Synchronous   |   |
| <b>Reentrancy</b>         | Reentrant   |   |
| <b>Parameters (in)</b>    | job   | JobID of the operation that caused the callback     |
|                           | result  | Contains the result of the cryptographic operation. |
| <b>Parameters (inout)</b> | None  |   |
| <b>Parameters (out)</b>   | None  |   |
| <b>Return value</b>       | None  |   |
| <b>Description</b>        | CSM notifies the application that a job has finished. The function name is configurable. The function name itself is derived from "{CsmJob/CsmJobPrimitive CallbackRef}/CsmCallbackFunc". |   |
| <b>Available via</b>      | Csm.h   |   |

](SRS\_BSW\_00359, SRS\_BSW\_00360)

[SWS\_Csm\_01090] [ Csm\_ApplicationCallbackNotification shall be called once at the end when an asynchronous job's call has been finished, i.e. the given operation mode has been completely processed, the job has been aborted due to an error or the the job has been cancelled. Thus, if a job's call processed multiple operation modes, i.e. CRYPTO\_OPERATIONMODE\_STREAMSTART or CRYPTO\_OPERATIONMODE\_SINGLECALL, Csm\_ApplicationCallbackNotification is called only once.

]()

[SWS\_Csm\_01095] [ The CSM shall call the application callback function if the following condition is met:

```
((ecuc(Csm/CsmJobs/CsmJob.CsmProcessingMode)) == CRYPTO_PROCESSING_ASYN) &&
(CsmJob/CsmJobInterfaceUsePort == CRYPTO_USE_FNC) &&
(CsmJob/CsmJobPrimitiveCallbackRef != 0)
```

For the service interface the callback service shall be called if the asynchronous processing is configured:

```
{ecuc(Csm/CsmJobs/CsmJob.CsmProcessingMode)} == CRYPTO_PROCESSING_ASYN) &&
(CsmJob/CsmJobInterfaceUsePort != CRYPTO_USE_FNC)
```

]()

## 8.5 Service Interface

This chapter is an addition to the specification of the Csm module. Whereas the other parts of the specification define the behavior and the C-interfaces of the corresponding basic software module, this chapter formally specifies the corresponding AUTOSAR service in terms of the SWC template. The interfaces described here will be visible on the VFB and are used to generate the RTE between application software and the Csm module.

### 8.5.1 Client-Server-Interfaces

#### 8.5.1.1 CsmKeyManagement\_{Key}

[SWS Csm\_01905]

|                        |  |                            |   |
|------------------------|--|----------------------------|---|
| <b>Name</b>            | CsmKeyManagement_{Key}   |                            |   |
| <b>Comment</b>         | Interface to execute the key management functions.   |                            |   |
| <b>IsService</b>       | true   |                            |   |
| <b>Variation</b>       | <pre>{ecuc(Csm/CsmKeys/CsmKey.CsmKeyUsePort)} == TRUE) Key = {ecuc(Csm/CsmKeys/CsmKey.SHORT-NAME)}</pre> |                            |   |
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 6  | CRYPTO_E_KEY_READ_FAIL     | The service request failed because read access was denied.  |
|                        | 7  | CRYPTO_E_KEY_WRITE_FAIL    | The service request failed because write access was denied.   |
|                        | 8  | CRYPTO_E_KEY_NOT_AVAILABLE | The service request failed because the key is not available.  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10   | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 13   | CRYPTO_E_KEY_              | The service request failed because of uninitialized source  |

|  |       |              |
|--|-------|--------------|
|  | EMPTY | key element. |
|--|-------|--------------|

|                        |  |   |
|------------------------|--|---|
| <b>Operation</b>       | KeyCopy  |   |
| <b>Comment</b>         | This function shall copy all key elements from the source key to a target key.   |   |
| <b>Variation</b>       | --   |   |
| <b>Parameters</b>      | targetKeyld  |   |
|                        | <b>Type</b>  | uint32  |
|                        | <b>Direction</b>   | IN  |
|                        | <b>Comment</b>   | Holds the identifier of the key whose key element shall be the destination element. |
|                        | <b>Variation</b>   | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_READ_FAIL<br>CRYPTO_E_KEY_WRITE_FAIL<br>CRYPTO_E_KEY_NOT_AVAILABLE<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |   |

|                        |   |   |
|------------------------|---|---|
| <b>Operation</b>       | KeyDerive   |   |
| <b>Comment</b>         | Derives a new key by using the key elements in the given key. The given key contains the key elements for the password and salt. The derived key is stored in the key element with the id 1 of the key identified by targetCryptoKeyld. |   |
| <b>Variation</b>       | --  |   |
| <b>Parameters</b>      | targetKeyld   |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Holds the identifier of the key which is used to store the derived key. |
|                        | <b>Variation</b>  | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_READ_FAIL<br>CRYPTO_E_KEY_WRITE_FAIL<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY  |   |

|                  |                |  |
|------------------|----------------|--|
| <b>Operation</b> | KeyElementCopy |  |
|------------------|----------------|--|

|                        |  |   |
|------------------------|--|---|
| <b>Comment</b>         | This function shall copy a key elements from one key to a target key   |   |
| <b>Variation</b>       | --   |   |
| <b>Parameters</b>      | keyElementId   |   |
|                        | <b>Type</b>  | uint32  |
|                        | <b>Direction</b>   | IN  |
|                        | <b>Comment</b>   | Holds the identifier of the key element which shall be the source for the copy operation. |
|                        | <b>Variation</b>   | --  |
|                        | targetKeyId  |   |
|                        | <b>Type</b>  | uint32  |
|                        | <b>Direction</b>   | IN  |
|                        | <b>Comment</b>   | Holds the identifier of the key whose key element shall be the destination element.       |
|                        | <b>Variation</b>   | --  |
|                        | targetKeyElementId   |   |
|                        | <b>Type</b>  | uint32  |
|                        | <b>Direction</b>   | IN  |
| <b>Comment</b>         | Holds the identifier of the key element which shall be the destination for the copy operation.   |   |
| <b>Variation</b>       | --   |   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_READ_FAIL<br>CRYPTO_E_KEY_WRITE_FAIL<br>CRYPTO_E_KEY_NOT_AVAILABLE<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |   |

|                   |   |   |
|-------------------|---|---|
| <b>Operation</b>  | KeyElementCopyPartial   |   |
| <b>Comment</b>    | This function shall copy parts of a a key elements from one key to parts of a target key element of a target key. |   |
| <b>Variation</b>  | --  |   |
| <b>Parameters</b> | keyElementId  |   |
|                   | <b>Type</b>   | uint32  |
|                   | <b>Direction</b>  | IN  |
|                   | <b>Comment</b>  | Holds the identifier of the key element which shall be the source for the |

|                        |                                   |   |
|------------------------|-----------------------------------|---|
|                        |                                   | copy operation.   |
|                        | <b>Variation</b>                  | --  |
|                        | keyElementSourceOffset            |   |
|                        | <b>Type</b>                       | uint32  |
|                        | <b>Direction</b>                  | IN  |
|                        | <b>Comment</b>                    | This is the offset of the source key element indicating the start index of the copy operation.      |
|                        | <b>Variation</b>                  | --  |
|                        | keyElementTargetOffset            |   |
|                        | <b>Type</b>                       | uint32  |
|                        | <b>Direction</b>                  | IN  |
|                        | <b>Comment</b>                    | This is the offset of the destination key element indicating the start index of the copy operation. |
|                        | <b>Variation</b>                  | --  |
|                        | keyElementCopyLength              |   |
|                        | <b>Type</b>                       | uint32  |
|                        | <b>Direction</b>                  | IN  |
|                        | <b>Comment</b>                    | Specifies the number of bytes that shall be copied.   |
|                        | <b>Variation</b>                  | --  |
|                        | targetKeyld                       |   |
|                        | <b>Type</b>                       | uint32  |
|                        | <b>Direction</b>                  | IN  |
|                        | <b>Comment</b>                    | Holds the identifier of the key whose key element shall be the destination element.                 |
|                        | <b>Variation</b>                  | --  |
|                        | targetKeyElementld                |   |
|                        | <b>Type</b>                       | uint32  |
|                        | <b>Direction</b>                  | IN  |
|                        | <b>Comment</b>                    | Holds the identifier of the key element which shall be the destination for the copy operation.      |
|                        | <b>Variation</b>                  | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY |   |

|  |   |
|--|---|
|  | CRYPTO_E_KEY_READ_FAIL<br>CRYPTO_E_KEY_WRITE_FAIL<br>CRYPTO_E_KEY_NOT_AVAILABLE<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |
|--|---|

|                        |   |  |
|------------------------|---|--|
| <b>Operation</b>       | KeyElementGet   |  |
| <b>Comment</b>         | Retrieves the key element bytes from a specific key element of the key and stores the key element in the provided buffer. |  |
| <b>Variation</b>       | --  |  |
| <b>Parameters</b>      | keyElementId  |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Holds the identifier of the key element to be read.    |
|                        | <b>Variation</b>  | --   |
|                        | keyPtr  |  |
|                        | <b>Type</b>   | Csm_KeyDataType_{Crypto}                               |
|                        | <b>Direction</b>  | OUT  |
|                        | <b>Comment</b>  | Holds the data to the key element bytes to be written. |
|                        | <b>Variation</b>  | --   |
|                        | keyLength   |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Contains the number of key element bytes.              |
| <b>Variation</b>       | --  |  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_READ_FAIL<br>CRYPTO_E_KEY_NOT_AVAILABLE<br>CRYPTO_E_KEY_EMPTY           |  |

|                   |  |
|-------------------|--|
| <b>Operation</b>  | KeyElementSet                                |
| <b>Comment</b>    | Sets the given key element bytes to the key. |
| <b>Variation</b>  | --   |
| <b>Parameters</b> | keyElementId                                 |

|                        |  |  |
|------------------------|--|--|
|                        | <b>Type</b>  | uint32   |
|                        | <b>Direction</b>   | IN   |
|                        | <b>Comment</b>   | Holds the identifier of the key element to be written.   |
|                        | <b>Variation</b>   | --   |
|                        | keyPtr   |  |
|                        | <b>Type</b>  | Csm_KeyDataType_{Crypto}                                 |
|                        | <b>Direction</b>   | IN   |
|                        | <b>Comment</b>   | Holds the data to the key element bytes to be processed. |
|                        | <b>Variation</b>   | --   |
|                        | keyLength  |  |
|                        | <b>Type</b>  | uint32   |
|                        | <b>Direction</b>   | IN   |
|                        | <b>Comment</b>   | Contains the number of key element bytes.                |
|                        | <b>Variation</b>   | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_WRITE_FAIL<br>CRYPTO_E_KEY_NOT_AVAILABLE<br>CRYPTO_E_KEY_SIZE_MISMATCH |  |

|                   |   |   |
|-------------------|---|---|
| <b>Operation</b>  | KeyExchangeCalcPubVal   |   |
| <b>Comment</b>    | Calculates the public value of the current user for the key exchange and stores the public key in the provided buffer |   |
| <b>Variation</b>  | --  |   |
| <b>Parameters</b> | publicValuePtr  |   |
|                   | <b>Type</b>   | Csm_KeyDataType_{Crypto}  |
|                   | <b>Direction</b>  | OUT   |
|                   | <b>Comment</b>  | Contains the pointer to the memory location where the public value shall be stored. |
|                   | <b>Variation</b>  | --  |
|                   | publicValueLengthPtr  |   |
|                   | <b>Type</b>   | uint32  |
|                   | <b>Direction</b>  | INOUT   |
| <b>Comment</b>    | Holds a pointer to the memory location in which the public value length in  |   |



|                        |   |   |
|------------------------|---|---|
|                        |   | bytes is stored. On calling this function, this parameter shall contain the size of the buffer in bytes provided by publicValuePtr. When the request has finished, the actual length of the returned value shall be stored. |
|                        | <b>Variation</b>  | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_EMPTY |   |

|                        |  |  |
|------------------------|--|--|
| <b>Operation</b>       | KeyExchangeCalcSecret  |  |
| <b>Comment</b>         | Calculates the shared secret key for the key exchange with the key material of the key identified by the keyId and the partner public key. The shared secret key is stored as a key element in the same key. |  |
| <b>Variation</b>       | --   |  |
| <b>Parameters</b>      | partnerPublicValuePtr  |  |
|                        | <b>Type</b>  | Csm_KeyDataType_{Crypto}   |
|                        | <b>Direction</b>   | IN   |
|                        | <b>Comment</b>   | Holds the pointer to the memory location containing the partner's public value |
|                        | <b>Variation</b>   | --   |
|                        | partnerPublicValueLength   |  |
|                        | <b>Type</b>  | uint32   |
|                        | <b>Direction</b>   | IN   |
|                        | <b>Comment</b>   | Contains the number of bytes of the partner public value                       |
|                        | <b>Variation</b>   | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_EMPTY  |  |

|                        |   |  |
|------------------------|---|--|
| <b>Operation</b>       | KeyGenerate   |  |
| <b>Comment</b>         | Generates new key material and store it in the key identified by keyId.           |  |
| <b>Variation</b>       | --  |  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_EMPTY |  |

|                        |  |
|------------------------|--|
| <b>Operation</b>       | KeySetValid                                  |
| <b>Comment</b>         | Sets the given key element bytes to the key. |
| <b>Variation</b>       | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY            |

|                        |   |  |
|------------------------|---|--|
| <b>Operation</b>       | RandomSeed  |  |
| <b>Comment</b>         | Feeds the key element CRYPTO_KE_RANDOM_SEED with a random seed.                   |  |
| <b>Variation</b>       | --  |  |
| <b>Parameters</b>      | seedPtr   |  |
|                        | <b>Type</b>   | Csm_KeyDataType_{Crypto}   |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Holds the data which shall be used for the random seed initialization. |
|                        | <b>Variation</b>  | --   |
|                        | seedLength  |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Contains the length of the seed in bytes.                              |
|                        | <b>Variation</b>  | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_EMPTY |  |

](SRS\_Csm\_00066)

### 8.5.1.2 CsmHash\_{PrimitiveCfg}

[SWS\_Csm\_00946]

|                  |   |
|------------------|---|
| <b>Name</b>      | CsmHash_{PrimitiveCfg}  |
| <b>Comment</b>   | Synchronous processing interface to execute the hash calculation.   |
| <b>IsService</b> | true  |
| <b>Variation</b> | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |

|                        |   |               |  |
|------------------------|---|---------------|--|
| <b>Possible Errors</b> | 0 | E_OK          | Operation successful                   |
|                        | 1 | E_NOT_OK      | Operation failed                       |
|                        | 2 | CRYPTO_E_BUSY | Request failed, service is still busy. |

|                        |   |  |  |
|------------------------|---|--|--|
| <b>Operation</b>       | Hash  |  |  |
| <b>Comment</b>         | Streaming approach of the hash calculation. |  |  |
| <b>Variation</b>       | --  |  |  |
| <b>Parameters</b>      | dataBuffer                                  |  |  |
|                        | <b>Type</b>                                 | Csm_HashDataType_{Crypto}                              |  |
|                        | <b>Direction</b>                            | IN   |  |
|                        | <b>Comment</b>                              | Contains the data to be hashed.                        |  |
|                        | <b>Variation</b>                            | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}           |  |
|                        | dataLength                                  |  |  |
|                        | <b>Type</b>                                 | uint32   |  |
|                        | <b>Direction</b>                            | IN   |  |
|                        | <b>Comment</b>                              | Contains the length in bytes of the data to be hashed. |  |
|                        | <b>Variation</b>                            | --   |  |
|                        | resultBuffer                                |  |  |
|                        | <b>Type</b>                                 | Csm_HashResultType_{Crypto}                            |  |
|                        | <b>Direction</b>                            | OUT  |  |
|                        | <b>Comment</b>                              | Contains the data of the hash.                         |  |
|                        | <b>Variation</b>                            | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}           |  |
|                        | resultLength                                |  |  |
| <b>Type</b>            | uint32                                      |  |  |
| <b>Direction</b>       | INOUT                                       |  |  |
| <b>Comment</b>         | Contains the length in bytes of the hash.   |  |  |
| <b>Variation</b>       | --  |  |  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY           |  |  |

](SRS\_CryptoStack\_00090)

### 8.5.1.3 CsmMacGenerate\_{PrimitiveCfg}

#### [SWS\_Csm\_09000]

|                        |   |                            |   |
|------------------------|---|----------------------------|---|
| <b>Name</b>            | CsmMacGenerate_{PrimitiveCfg}   |                            |   |
| <b>Comment</b>         | Synchronous processing interface to execute the MAC generation.   |                            |   |
| <b>IsService</b>       | true  |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0   | E_OK                       | Operation successful  |
|                        | 1   | E_NOT_OK                   | Operation failed  |
|                        | 2   | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10  | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 13  | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                   |  |  |  |
|-------------------|--|--|--|
| <b>Operation</b>  | MacGenerate  |  |  |
| <b>Comment</b>    | Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer. |  |  |
| <b>Variation</b>  | --   |  |  |
| <b>Parameters</b> | dataBuffer   |  |  |
|                   | <b>Type</b>  | Csm_MacGenerateDataType_{Crypto}   |  |
|                   | <b>Direction</b>   | IN   |  |
|                   | <b>Comment</b>   | Contains the data from which a MAC shall be generated of.                        |  |
|                   | <b>Variation</b>   | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                                     |  |
|                   | dataLength   |  |  |
|                   | <b>Type</b>  | uint32   |  |
|                   | <b>Direction</b>   | IN   |  |
|                   | <b>Comment</b>   | Contains the length in bytes of the data from which a MAC shall be generated of. |  |
|                   | <b>Variation</b>   | --   |  |
| resultBuffer      |  |  |  |
| <b>Type</b>       | Csm_MacGenerateResultType_{Crypto}   |  |  |

|                        |   |  |
|------------------------|---|--|
|                        | <b>Direction</b>  | OUT  |
|                        | <b>Comment</b>  | Contains the data of the MAC.                |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME} |
|                        | resultLength  |  |
|                        | <b>Type</b>   | uint32                                       |
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Contains the length in bytes of the MAC.     |
|                        | <b>Variation</b>  | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |  |

](SRS\_CryptoStack\_00090)

#### 8.5.1.4 CsmMacVerify\_{PrimitiveCfg}

[SWS\_Csm\_00936]

|                        |   |                            |   |
|------------------------|---|----------------------------|---|
| <b>Name</b>            | CsmMacVerify_{PrimitiveCfg}   |                            |   |
| <b>Comment</b>         | Synchronous processing interface to execute the MAC verification.   |                            |   |
| <b>IsService</b>       | true  |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0   | E_OK                       | Operation successful  |
|                        | 1   | E_NOT_OK                   | Operation failed  |
|                        | 2   | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10  | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 13  | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                  |  |
|------------------|--|
| <b>Operation</b> | MacVerify  |
| <b>Comment</b>   | Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer. |

|                        |   |  |
|------------------------|---|--|
| <b>Variation</b>       | --  |  |
| <b>Parameters</b>      | dataBuffer  |  |
|                        | <b>Type</b>   | Csm_MacVerifyDataType_{Crypto}   |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Contains the data from which a MAC shall be generated of.                  |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                               |
|                        | dataLength  |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Contains the length in bytes of the data for whichs MAC shall be verified. |
|                        | <b>Variation</b>  | --   |
|                        | compareBuffer   |  |
|                        | <b>Type</b>   | Csm_MacVerifyCompareType_{Crypto}  |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Contains the MAC to be verified.   |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                               |
|                        | compareLength   |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Contains the length in BITS of the MAC to be verified.                     |
|                        | <b>Variation</b>  | --   |
| resultBuffer           |   |  |
| <b>Type</b>            | Crypto_VerifyResultType   |  |
| <b>Direction</b>       | OUT   |  |
| <b>Comment</b>         | Contains the verification result.   |  |
| <b>Variation</b>       | --  |  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |  |

### 8.5.1.5 CsmEncrypt\_{PrimitiveCfg}

#### [SWS\_Csm\_00947]

|                        |   |                            |   |
|------------------------|---|----------------------------|---|
| <b>Name</b>            | CsmEncrypt_{PrimitiveCfg}   |                            |   |
| <b>Comment</b>         | Synchronous processing interface to execute the encryption.   |                            |   |
| <b>IsService</b>       | true  |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0   | E_OK                       | Operation successful  |
|                        | 1   | E_NOT_OK                   | Operation failed  |
|                        | 2   | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10  | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 13  | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                   |  |   |  |
|-------------------|--|---|--|
| <b>Operation</b>  | Encrypt  |   |  |
| <b>Comment</b>    | Encrypts the given data and store the ciphertext in the memory location pointed by the result pointer. |   |  |
| <b>Variation</b>  | --   |   |  |
| <b>Parameters</b> | dataBuffer   |   |  |
|                   | <b>Type</b>  | Csm_EncryptDataType_{Crypto}                              |  |
|                   | <b>Direction</b>   | IN  |  |
|                   | <b>Comment</b>   | Contains the data to be encrypted.                        |  |
|                   | <b>Variation</b>   | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}              |  |
|                   | dataLength   |   |  |
|                   | <b>Type</b>  | uint32  |  |
|                   | <b>Direction</b>   | IN  |  |
|                   | <b>Comment</b>   | Contains the length in bytes of the data to be encrypted. |  |
|                   | <b>Variation</b>   | --  |  |
|                   | result   |   |  |
|                   | <b>Type</b>  | Csm_EncryptResultType_{Crypto}                            |  |

|                        |   |  |
|------------------------|---|--|
|                        | <b>Direction</b>  | OUT  |
|                        | <b>Comment</b>  | Contains the data of the cipher.             |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME} |
|                        | resultLength  |  |
|                        | <b>Type</b>   | uint32                                       |
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Contains the length in bytes of the cipher.  |
|                        | <b>Variation</b>  | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |  |

](SRS\_CryptoStack\_00906)

### 8.5.1.6 CsmDecrypt\_{PrimitiveCfg}

[SWS\_Csm\_01906][

|                        |  |                            |   |
|------------------------|--|----------------------------|---|
| <b>Name</b>            | CsmDecrypt_{PrimitiveCfg}  |                            |   |
| <b>Comment</b>         | Synchronous processing interface to execute the decryption.  |                            |   |
| <b>IsService</b>       | true   |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive})/{Primitive}Config.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10   | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 13   | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                  |                                       |
|------------------|---------------------------------------|
| <b>Operation</b> | Decrypt                               |
| <b>Comment</b>   | Streaming approach of the decryption. |



|                        |   |   |
|------------------------|---|---|
| <b>Variation</b>       | --  |   |
| <b>Parameters</b>      | dataBuffer  |   |
|                        | <b>Type</b>   | Csm_DecryptDataType_{Crypto}                              |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the data to be decrypted.                        |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}              |
|                        | dataLength  |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data to be decrypted. |
|                        | <b>Variation</b>  | --  |
|                        | resultBuffer  |   |
|                        | <b>Type</b>   | Csm_DecryptResultType_{Crypto}                            |
|                        | <b>Direction</b>  | OUT   |
|                        | <b>Comment</b>  | Contains the data of the decrypted plaintext.             |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}              |
|                        | resultLength  |   |
| <b>Type</b>            | uint32  |   |
| <b>Direction</b>       | INOUT   |   |
| <b>Comment</b>         | Contains the length in bytes of the decrypted plaintext.  |   |
| <b>Variation</b>       | --  |   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |   |

](SRS\_CryptoStack\_00090)

### 8.5.1.7 CsmAEADEncrypt\_{PrimitiveCfg}

[SWS\_Csm\_01910]

|                |  |
|----------------|--|
| <b>Name</b>    | CsmAEADEncrypt_{PrimitiveCfg}                                    |
| <b>Comment</b> | Synchronous processing interface to execute the AEAD encryption. |

|                        |   |                            |   |
|------------------------|---|----------------------------|---|
| <b>IsService</b>       | true  |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0   | E_OK                       | Operation successful  |
|                        | 1   | E_NOT_OK                   | Operation failed  |
|                        | 2   | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10  | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 13  | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                      |  |  |  |
|----------------------|--|--|--|
| <b>Operation</b>     | AEADEncrypt                                |  |  |
| <b>Comment</b>       | Streaming approach of the AEAD encryption. |  |  |
| <b>Variation</b>     | --   |  |  |
| <b>Parameters</b>    | plaintextBuffer                            |  |  |
|                      | <b>Type</b>                                | Csm_AEADEncryptPlaintextType_{Crypto}  |  |
|                      | <b>Direction</b>                           | IN   |  |
|                      | <b>Comment</b>                             | Contains the plaintext to be encrypted with AEAD.  |  |
|                      | <b>Variation</b>                           | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |  |
|                      | plaintextLength                            |  |  |
|                      | <b>Type</b>                                | uint32   |  |
|                      | <b>Direction</b>                           | IN   |  |
|                      | <b>Comment</b>                             | This element Contains the length in bytes of the plaintext to be encrypted with AEAD.    |  |
|                      | <b>Variation</b>                           | --   |  |
|                      | associatedDataBuffer                       |  |  |
|                      | <b>Type</b>                                | Csm_AEADEncryptAssociatedDataType_{Crypto}   |  |
|                      | <b>Direction</b>                           | IN   |  |
|                      | <b>Comment</b>                             | Contains the data of the header (that is not part of the encryption but authentication). |  |
|                      | <b>Variation</b>                           | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |  |
| associatedDataLength |  |  |  |

|                        |   |  |
|------------------------|---|--|
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Contains the length in bytes of the data of the header.      |
|                        | <b>Variation</b>  | --   |
|                        | ciphertextBuffer  |  |
|                        | <b>Type</b>   | Csm_AEADEncryptCiphertextType_{Crypto}                       |
|                        | <b>Direction</b>  | OUT  |
|                        | <b>Comment</b>  | Contains the data of the AEAD cipher.                        |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                 |
|                        | ciphertextLengthPtr   |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data of the AEAD cipher. |
|                        | <b>Variation</b>  | --   |
|                        | tagBuffer   |  |
|                        | <b>Type</b>   | Csm_AEADEncryptTagType_{Crypto}                              |
|                        | <b>Direction</b>  | OUT  |
|                        | <b>Comment</b>  | Contains the data of the Tag.                                |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                 |
|                        | tagLength   |  |
| <b>Type</b>            | uint32  |  |
| <b>Direction</b>       | INOUT   |  |
| <b>Comment</b>         | Contains the length in bytes of the data of the Tag.  |  |
| <b>Variation</b>       | --  |  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |  |

](SRS\_CryptoStack\_00090)

### 8.5.1.8 CsmAEADDecrypt\_{PrimitiveCfg}

[SWS\_Csm\_01915][

|                        |   |                            |   |
|------------------------|---|----------------------------|---|
| <b>Name</b>            | CsmAEADDecrypt_{PrimitiveCfg}   |                            |   |
| <b>Comment</b>         | Synchronous processing interface to execute the AEAD decryption.  |                            |   |
| <b>IsService</b>       | true  |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0   | E_OK                       | Operation successful  |
|                        | 1   | E_NOT_OK                   | Operation failed  |
|                        | 2   | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10  | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 13  | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                   |   |   |
|-------------------|---|---|
| <b>Operation</b>  | AEADDecrypt   |   |
| <b>Comment</b>    | Streaming approach of the AEAD decryption.  |   |
| <b>Variation</b>  | --  |   |
| <b>Parameters</b> | ciphertextBuffer  |   |
|                   | <b>Type</b>   | Csm_AEADDecryptCiphertextType_{Crypto}                                    |
|                   | <b>Direction</b>  | IN  |
|                   | <b>Comment</b>  | Contains the ciphertext to be decrypted with AEAD.                        |
|                   | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                              |
|                   | ciphertextLength  |   |
|                   | <b>Type</b>   | uint32  |
|                   | <b>Direction</b>  | IN  |
|                   | <b>Comment</b>  | Contains the length in bytes of the ciphertext to be decrypted with AEAD. |
|                   | <b>Variation</b>  | --  |
|                   | associatedDataBuffer  |   |
|                   | <b>Type</b>   | Csm_AEADDecryptAssociatedDataType_{Crypto}                                |
|                   | <b>Direction</b>  | IN  |
| <b>Comment</b>    | Contains the data of the header (that is not part of the encryption but authentication) . |   |

|                      |   |
|----------------------|---|
| <b>Variation</b>     | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                              |
| associatedDataLength |   |
| <b>Type</b>          | uint32  |
| <b>Direction</b>     | IN  |
| <b>Comment</b>       | Contains the length in bytes of the data of the header.                   |
| <b>Variation</b>     | --  |
| tagBuffer            |   |
| <b>Type</b>          | Csm_AEADDecryptTagType_{Crypto}   |
| <b>Direction</b>     | IN  |
| <b>Comment</b>       | Contains the data of the Tag.   |
| <b>Variation</b>     | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                              |
| tagLength            |   |
| <b>Type</b>          | uint32  |
| <b>Direction</b>     | IN  |
| <b>Comment</b>       | Contains the length in BITS of the data of the Tag.                       |
| <b>Variation</b>     | --  |
| plaintextBuffer      |   |
| <b>Type</b>          | Csm_AEADDecryptPlaintextType_{Crypto}                                     |
| <b>Direction</b>     | OUT   |
| <b>Comment</b>       | Contains the data of the decrypted AEAD plaintext.                        |
| <b>Variation</b>     | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                              |
| plaintextLength      |   |
| <b>Type</b>          | uint32  |
| <b>Direction</b>     | INOUT   |
| <b>Comment</b>       | Contains the length in bytes of the data of the decrypted AEAD plaintext. |
| <b>Variation</b>     | --  |
| resultBuffer         |   |
| <b>Type</b>          | Crypto_VerifyResultType   |
| <b>Direction</b>     | OUT   |
| <b>Comment</b>       | Contains the verification result.   |

|                        |   |    |
|------------------------|---|----|
|                        | <b>Variation</b>  | -- |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |    |

](SRS\_CryptoStack\_00090)

### 8.5.1.9 CsmSignatureGenerate\_{PrimitiveCfg}

[SWS\_Csm\_00903]

|                        |   |                            |   |
|------------------------|---|----------------------------|---|
| <b>Name</b>            | CsmSignatureGenerate_{PrimitiveCfg}   |                            |   |
| <b>Comment</b>         | Synchronous processing interface to generate a signature.   |                            |   |
| <b>IsService</b>       | true  |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0   | E_OK                       | Operation successful  |
|                        | 1   | E_NOT_OK                   | Operation failed  |
|                        | 2   | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10  | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 13  | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                   |   |  |
|-------------------|---|--|
| <b>Operation</b>  | SignatureGenerate                               |  |
| <b>Comment</b>    | Streaming approach of the signature generation. |  |
| <b>Variation</b>  | --  |  |
| <b>Parameters</b> | dataBuffer                                      |  |
|                   | <b>Type</b>                                     | Csm_SignatureGenerateDataType_{Crypto}                         |
|                   | <b>Direction</b>                                | IN   |
|                   | <b>Comment</b>                                  | Contains the data from which the signature shall be generated. |
|                   | <b>Variation</b>                                | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                   |
|                   | dataLength                                      |  |

|                        |   |   |
|------------------------|---|---|
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data from which the signature shall be generated. |
|                        | <b>Variation</b>  | --  |
|                        | resultBuffer  |   |
|                        | <b>Type</b>   | Csm_SignatureGenerateResultType_{Crypto}  |
|                        | <b>Direction</b>  | OUT   |
|                        | <b>Comment</b>  | Contains the signature.   |
|                        | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |
|                        | resultLength  |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | INOUT   |
|                        | <b>Comment</b>  | Contains the length in bytes of the signature.  |
|                        | <b>Variation</b>  | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |   |

](SRS\_CryptoStack\_00090)

### 8.5.1.10 CsmSignatureVerify\_{PrimitiveCfg}

[SWS\_Csm\_00943]

|                        |   |                        |  |
|------------------------|---|------------------------|--|
| <b>Name</b>            | CsmSignatureVerify_{PrimitiveCfg}   |                        |  |
| <b>Comment</b>         | Synchronous processing interface to execute the signature verification.   |                        |  |
| <b>IsService</b>       | true  |                        |  |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                        |  |
| <b>Possible Errors</b> | 0   | E_OK                   | Operation successful                   |
|                        | 1   | E_NOT_OK               | Operation failed                       |
|                        | 2   | CRYPTO_E_BUSY          | Request failed, service is still busy. |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID | Request failed, the key is not valid.  |

|  |    |                            |   |
|--|----|----------------------------|---|
|  | 10 | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|  | 13 | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                   |                                  |  |  |
|-------------------|----------------------------------|--|--|
| <b>Operation</b>  | SignatureVerify                  |  |  |
| <b>Comment</b>    | Interface to verify a signature. |  |  |
| <b>Variation</b>  | --                               |  |  |
| <b>Parameters</b> | dataBuffer                       |  |  |
|                   | <b>Type</b>                      | Csm_SignatureVerifyDataType_{Crypto}   |  |
|                   | <b>Direction</b>                 | IN   |  |
|                   | <b>Comment</b>                   | Contains the data for whichs signature shall be verified.                        |  |
|                   | <b>Variation</b>                 | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                                     |  |
|                   | dataLength                       |  |  |
|                   | <b>Type</b>                      | uint32   |  |
|                   | <b>Direction</b>                 | IN   |  |
|                   | <b>Comment</b>                   | Contains the length in bytes of the data for whichs signature shall be verified. |  |
|                   | <b>Variation</b>                 | --   |  |
|                   | compareBuffer                    |  |  |
|                   | <b>Type</b>                      | Csm_SignatureVerifyCompareType_{Crypto}  |  |
|                   | <b>Direction</b>                 | IN   |  |
|                   | <b>Comment</b>                   | Contains the signature to be verified.   |  |
|                   | <b>Variation</b>                 | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}                                     |  |
|                   | compareLength                    |  |  |
|                   | <b>Type</b>                      | uint32   |  |
|                   | <b>Direction</b>                 | IN   |  |
|                   | <b>Comment</b>                   | Contains the length in bytes of the signature to be verified.                    |  |
|                   | <b>Variation</b>                 | --   |  |
| resultBuffer      |                                  |  |  |
| <b>Type</b>       | Crypto_VerifyResultType          |  |  |
| <b>Direction</b>  | OUT                              |  |  |



|                        |   |                                   |
|------------------------|---|-----------------------------------|
|                        | <b>Comment</b>  | Contains the verification result. |
|                        | <b>Variation</b>  | --                                |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |                                   |

](SRS\_CryptoStack\_00090)

### 8.5.1.11 CsmRandomGenerate\_{PrimitiveCfg}

[SWS\_Csm\_00902]

|                        |   |                            |  |
|------------------------|---|----------------------------|--|
| <b>Name</b>            | CsmRandomGenerate_{PrimitiveCfg}  |                            |  |
| <b>Comment</b>         | Synchronous processing interface to execute the random number generation.   |                            |  |
| <b>IsService</b>       | true  |                            |  |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                            |  |
| <b>Possible Errors</b> | 0   | E_OK                       | Operation successful   |
|                        | 1   | E_NOT_OK                   | Operation failed   |
|                        | 2   | CRYPTO_E_BUSY              | Request failed, service is still busy.                           |
|                        | 4   | CRYPTO_E_ENTROPY_EXHAUSTED | Request failed, entropy of random number generator is exhausted. |

|                   |   |  |
|-------------------|---|--|
| <b>Operation</b>  | RandomGenerate  |  |
| <b>Comment</b>    | Synchronous processing interface to execute the random number generation. |  |
| <b>Variation</b>  | --  |  |
| <b>Parameters</b> | resultBuffer  |  |
|                   | <b>Type</b>   | Csm_RandomGenerateResultType_{Crypto}        |
|                   | <b>Direction</b>  | OUT  |
|                   | <b>Comment</b>  | Contains the random number                   |
|                   | <b>Variation</b>  | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME} |
|                   | resultLength  |  |
|                   | <b>Type</b>   | uint32                                       |
|                   | <b>Direction</b>  | INOUT  |

|                        |   |  |
|------------------------|---|--|
|                        | <b>Comment</b>  | Contains the length in bytes of the data of random number. |
|                        | <b>Variation</b>  | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_ENTROPY_EXHAUSTED |  |

](SRS\_CryptoStack\_00090)

## 8.5.2 Client-Server-Interfaces (DATA\_REFERENCES)

### 8.5.2.1 CsmHash

[SWS\_Csm\_91051]

|                        |  |                       |   |
|------------------------|--|-----------------------|---|
| <b>Name</b>            | CsmHash  |                       |   |
| <b>Comment</b>         | Asynchronous processing interface to execute the hash calculation. |                       |   |
| <b>IsService</b>       | true   |                       |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}                   |                       |   |
| <b>Possible Errors</b> | 0  | E_OK                  | Operation successful                              |
|                        | 1  | E_NOT_OK              | Operation failed                                  |
|                        | 2  | CRYPTO_E_BUSY         | Request failed, service is still busy.            |
|                        | 12   | CRYPTO_E_JOB_CANCELED | Request failed because the job has been canceled. |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                   |                                  |             |
|-------------------|----------------------------------|-------------|
| <b>Operation</b>  | Hash                             |             |
| <b>Comment</b>    | Utilize the random seed service. |             |
| <b>Variation</b>  | --                               |             |
| <b>Parameters</b> | dataBuffer                       |             |
|                   | <b>Type</b>                      | Csm_DataPtr |
|                   | <b>Direction</b>                 | IN          |

|                        |                                   |  |
|------------------------|-----------------------------------|--|
|                        | <b>Comment</b>                    | References the data to be hashed.                      |
|                        | <b>Variation</b>                  | --   |
|                        | dataLength                        |  |
|                        | <b>Type</b>                       | uint32   |
|                        | <b>Direction</b>                  | IN   |
|                        | <b>Comment</b>                    | Contains the length in bytes of the data to be hashed. |
|                        | <b>Variation</b>                  | --   |
|                        | resultBuffer                      |  |
|                        | <b>Type</b>                       | Csm_DataPtr  |
|                        | <b>Direction</b>                  | IN   |
|                        | <b>Comment</b>                    | References the data of the hash.                       |
|                        | <b>Variation</b>                  | --   |
|                        | resultLength                      |  |
|                        | <b>Type</b>                       | uint32   |
|                        | <b>Direction</b>                  | INOUT  |
|                        | <b>Comment</b>                    | Contains the length in bytes of the hash.              |
| <b>Variation</b>       | --                                |  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY |  |

](SRS\_CryptoStack\_00090)

### 8.5.2.2 CsmMacGenerate

[SWS\_Csm\_91052]

|                        |  |                        |  |
|------------------------|--|------------------------|--|
| <b>Name</b>            | CsmMacGenerate   |                        |  |
| <b>Comment</b>         | Asynchronous processing interface to execute the MAC generation. |                        |  |
| <b>IsService</b>       | true   |                        |  |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}                 |                        |  |
| <b>Possible Errors</b> | 0  | E_OK                   | Operation successful                   |
|                        | 1  | E_NOT_OK               | Operation failed                       |
|                        | 2  | CRYPTO_E_BUSY          | Request failed, service is still busy. |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID | Request failed, the key is not valid.  |

|  |    |                            |   |
|--|----|----------------------------|---|
|  | 10 | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|  | 12 | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|  | 13 | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                   |  |  |
|-------------------|--|--|
| <b>Operation</b>  | MacGenerate  |  |
| <b>Comment</b>    | Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer. |  |
| <b>Variation</b>  | --   |  |
| <b>Parameters</b> | dataBuffer   |  |
|                   | <b>Type</b>  | Csm_DataPtr  |
|                   | <b>Direction</b>   | IN   |
|                   | <b>Comment</b>   | References the data from which a MAC shall be generated of.                      |
|                   | <b>Variation</b>   | --   |
|                   | dataLength   |  |
|                   | <b>Type</b>  | uint32   |
|                   | <b>Direction</b>   | IN   |
|                   | <b>Comment</b>   | Contains the length in bytes of the data from which a MAC shall be generated of. |
|                   | <b>Variation</b>   | --   |
|                   | resultBuffer   |  |
|                   | <b>Type</b>  | Csm_DataPtr  |
|                   | <b>Direction</b>   | OUT  |
|                   | <b>Comment</b>   | References the data of the MAC.  |
| <b>Variation</b>  | --   |  |

|                        |   |  |
|------------------------|---|--|
|                        | resultLength  |  |
|                        | <b>Type</b>   | uint32                                   |
|                        | <b>Direction</b>  | INOUT                                    |
|                        | <b>Comment</b>  | Contains the length in bytes of the MAC. |
|                        | <b>Variation</b>  | --                                       |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |  |

](SRS\_CryptoStack\_00090)

### 8.5.2.3 CsmMacVerify

[SWS\_Csm\_91053]

|                        |  |                            |   |
|------------------------|--|----------------------------|---|
| <b>Name</b>            | CsmMacVerify   |                            |   |
| <b>Comment</b>         | Asynchronous processing interface to execute the MAC verification. |                            |   |
| <b>IsService</b>       | true   |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}                   |                            |   |
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10   | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 12   | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|                        | 13   | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                        |                  |
|------------------------|------------------|
| <b>Operation</b>       | CancelJob        |
| <b>Comment</b>         | Cancels the job. |
| <b>Variation</b>       | --               |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK |

|  |                       |
|--|-----------------------|
|  | CRYPTO_E_JOB_CANCELED |
|--|-----------------------|

|                   |  |  |
|-------------------|--|--|
| <b>Operation</b>  | MacVerify  |  |
| <b>Comment</b>    | Uses the given data to perform a MAC generation and stores the MAC in the memory location pointed to by the MAC pointer. |  |
| <b>Variation</b>  | --   |  |
| <b>Parameters</b> | dataBuffer   |  |
|                   | <b>Type</b>  | Csm_DataPtr  |
|                   | <b>Direction</b>   | IN   |
|                   | <b>Comment</b>   | References the data from which a MAC shall be generated of.                |
|                   | <b>Variation</b>   | --   |
|                   | dataLength   |  |
|                   | <b>Type</b>  | uint32   |
|                   | <b>Direction</b>   | IN   |
|                   | <b>Comment</b>   | Contains the length in bytes of the data for whichs MAC shall be verified. |
|                   | <b>Variation</b>   | --   |
|                   | compareBuffer  |  |
|                   | <b>Type</b>  | Csm_DataPtr  |
|                   | <b>Direction</b>   | IN   |
|                   | <b>Comment</b>   | References the MAC to be verified.   |
|                   | <b>Variation</b>   | --   |
|                   | compareLength  |  |
|                   | <b>Type</b>  | uint32   |
|                   | <b>Direction</b>   | IN   |
|                   | <b>Comment</b>   | Contains the length in BITS of the MAC to be verified.                     |
|                   | <b>Variation</b>   | --   |
|                   | resultBuffer   |  |
|                   | <b>Type</b>  | Crypto_VerifyResultType  |
|                   | <b>Direction</b>   | OUT  |
|                   | <b>Comment</b>   | Contains the verification result.  |
| <b>Variation</b>  | --   |  |

|                        |   |
|------------------------|---|
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |
|------------------------|---|

](SRS\_CryptoStack\_00090)

### 8.5.2.4 CsmEncrypt

[SWS\_Csm\_91054]

|                        |  |                            |   |
|------------------------|--|----------------------------|---|
| <b>Name</b>            | CsmEncrypt   |                            |   |
| <b>Comment</b>         | Asynchronous processing interface to execute the encryption. |                            |   |
| <b>IsService</b>       | true   |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}             |                            |   |
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10   | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 12   | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|                        | 13   | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                  |   |
|------------------|---|
| <b>Operation</b> | Encrypt   |
| <b>Comment</b>   | Encrypts the given data and stores the ciphertext in the memory location pointed by the result pointer. |
| <b>Variation</b> | --  |

|                        |   |   |
|------------------------|---|---|
| <b>Parameters</b>      | dataBuffer  |   |
|                        | <b>Type</b>   | Csm_DataPtr   |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | References the data to be encrypted.                      |
|                        | <b>Variation</b>  | --  |
|                        | dataLength  |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data to be encrypted. |
|                        | <b>Variation</b>  | --  |
|                        | result  |   |
|                        | <b>Type</b>   | Csm_DataPtr   |
|                        | <b>Direction</b>  | OUT   |
|                        | <b>Comment</b>  | References the data of the cipher.                        |
|                        | <b>Variation</b>  | --  |
|                        | resultLength  |   |
| <b>Type</b>            | uint32  |   |
| <b>Direction</b>       | INOUT   |   |
| <b>Comment</b>         | Contains the length in bytes of the cipher.   |   |
| <b>Variation</b>       | --  |   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |   |

](SRS\_CryptoStack\_00090)

### 8.5.2.5 CsmDecrypt

[SWS\_Csm\_91055]

|                  |  |
|------------------|--|
| <b>Name</b>      | CsmDecrypt   |
| <b>Comment</b>   | Asynchronous processing interface to execute the decryption. |
| <b>IsService</b> | true   |



|                        |  |                            |   |
|------------------------|--|----------------------------|---|
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10   | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 12   | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|                        | 13   | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                   |  |   |
|-------------------|--|---|
| <b>Operation</b>  | Decrypt  |   |
| <b>Comment</b>    | Decrypts the given data and stores the plaintext in the memory location pointed by the resultBuffer pointer. |   |
| <b>Variation</b>  | --   |   |
| <b>Parameters</b> | dataBuffer   |   |
|                   | <b>Type</b>  | Csm_DataPtr   |
|                   | <b>Direction</b>   | IN  |
|                   | <b>Comment</b>   | References the data to be decrypted.                      |
|                   | <b>Variation</b>   | --  |
|                   | dataLength   |   |
|                   | <b>Type</b>  | uint32  |
|                   | <b>Direction</b>   | IN  |
|                   | <b>Comment</b>   | Contains the length in bytes of the data to be decrypted. |
|                   | <b>Variation</b>   | --  |

|                        |   |  |
|------------------------|---|--|
|                        | resultBuffer  |  |
|                        | <b>Type</b>   | Csm_DataPtr  |
|                        | <b>Direction</b>  | OUT  |
|                        | <b>Comment</b>  | References the data of the decrypted plaintext.          |
|                        | <b>Variation</b>  | --   |
|                        | resultLength  |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Contains the length in bytes of the decrypted plaintext. |
|                        | <b>Variation</b>  | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |  |

](SRS\_CryptoStack\_00090)

### 8.5.2.6 CsmAEADEncrypt

[SWS\_Csm\_91056]

|                        |   |                            |   |
|------------------------|---|----------------------------|---|
| <b>Name</b>            | CsmAEADEncrypt  |                            |   |
| <b>Comment</b>         | Asynchronous processing interface to execute the AEAD encryption. |                            |   |
| <b>IsService</b>       | true  |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}                  |                            |   |
| <b>Possible Errors</b> | 0   | E_OK                       | Operation successful  |
|                        | 1   | E_NOT_OK                   | Operation failed  |
|                        | 2   | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10  | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 12  | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|                        | 13  | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                     |  |  |
|---------------------|--|--|
| <b>Operation</b>    | AEADEncrypt                                |  |
| <b>Comment</b>      | Streaming approach of the AEAD encryption. |  |
| <b>Variation</b>    | --   |  |
| <b>Parameters</b>   | plaintextBuffer                            |  |
|                     | <b>Type</b>                                | Csm_DataPtr  |
|                     | <b>Direction</b>                           | IN   |
|                     | <b>Comment</b>                             | References the plaintext to be encrypted with AEAD.  |
|                     | <b>Variation</b>                           | --   |
|                     | plaintextLength                            |  |
|                     | <b>Type</b>                                | uint32   |
|                     | <b>Direction</b>                           | IN   |
|                     | <b>Comment</b>                             | This element Contains the length in bytes of the plaintext to be encrypted with AEAD.      |
|                     | <b>Variation</b>                           | --   |
|                     | associatedDataBuffer                       |  |
|                     | <b>Type</b>                                | Csm_DataPtr  |
|                     | <b>Direction</b>                           | IN   |
|                     | <b>Comment</b>                             | References the data of the header (that is not part of the encryption but authentication). |
|                     | <b>Variation</b>                           | --   |
|                     | associatedDataLength                       |  |
|                     | <b>Type</b>                                | uint32   |
|                     | <b>Direction</b>                           | IN   |
|                     | <b>Comment</b>                             | Contains the length in bytes of the data of the header.                                    |
|                     | <b>Variation</b>                           | --   |
| ciphertextBuffer    |  |  |
| <b>Type</b>         | Csm_DataPtr                                |  |
| <b>Direction</b>    | OUT  |  |
| <b>Comment</b>      | References the data of the AEAD cipher.    |  |
| <b>Variation</b>    | --   |  |
| ciphertextLengthPtr |  |  |

|                        |   |  |
|------------------------|---|--|
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data of the AEAD cipher. |
|                        | <b>Variation</b>  | --   |
|                        | tagBuffer   |  |
|                        | <b>Type</b>   | Csm_DataPtr  |
|                        | <b>Direction</b>  | OUT  |
|                        | <b>Comment</b>  | References the data of the Tag.                              |
|                        | <b>Variation</b>  | --   |
|                        | tagLength   |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data of the Tag.         |
|                        | <b>Variation</b>  | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |  |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

](SRS\_CryptoStack\_00090)

### 8.5.2.7 CsmAEADDecrypt

[SWS\_Csm\_91057]

|                  |   |
|------------------|---|
| <b>Name</b>      | CsmAEADDecrypt  |
| <b>Comment</b>   | Asynchronous processing interface to execute the AEAD decryption. |
| <b>IsService</b> | true  |
| <b>Variation</b> | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}                  |

|                        |    |                            |   |
|------------------------|----|----------------------------|---|
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10 | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 12 | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|                        | 13 | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                      |  |  |
|----------------------|--|--|
| <b>Operation</b>     | AEADDecrypt                                |  |
| <b>Comment</b>       | Streaming approach of the AEAD decryption. |  |
| <b>Variation</b>     | --   |  |
| <b>Parameters</b>    | ciphertextBuffer                           |  |
|                      | <b>Type</b>                                | Csm_DataPtr  |
|                      | <b>Direction</b>                           | IN   |
|                      | <b>Comment</b>                             | References the ciphertext to be decrypted with AEAD.                                       |
|                      | <b>Variation</b>                           | --   |
|                      | ciphertextLength                           |  |
|                      | <b>Type</b>                                | uint32   |
|                      | <b>Direction</b>                           | IN   |
|                      | <b>Comment</b>                             | Contains the length in bytes of the ciphertext to be decrypted with AEAD.                  |
|                      | <b>Variation</b>                           | --   |
|                      | associatedDataBuffer                       |  |
|                      | <b>Type</b>                                | Csm_DataPtr  |
|                      | <b>Direction</b>                           | IN   |
|                      | <b>Comment</b>                             | References the data of the header (that is not part of the encryption but authentication). |
|                      | <b>Variation</b>                           | --   |
| associatedDataLength |  |  |
| <b>Type</b>          | uint32                                     |  |

|                        |   |   |
|------------------------|---|---|
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data of the header.                   |
|                        | <b>Variation</b>  | --  |
|                        | tagBuffer   |   |
|                        | <b>Type</b>   | Csm_DataPtr   |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | References the data of the Tag.   |
|                        | <b>Variation</b>  | --  |
|                        | tagLength   |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the length in BITS of the data of the Tag.                       |
|                        | <b>Variation</b>  | --  |
|                        | plaintextBuffer   |   |
|                        | <b>Type</b>   | Csm_DataPtr   |
|                        | <b>Direction</b>  | OUT   |
|                        | <b>Comment</b>  | References the data of the decrypted AEAD plaintext.                      |
|                        | <b>Variation</b>  | --  |
|                        | plaintextLength   |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | INOUT   |
|                        | <b>Comment</b>  | Contains the length in bytes of the data of the decrypted AEAD plaintext. |
|                        | <b>Variation</b>  | --  |
|                        | resultBuffer  |   |
|                        | <b>Type</b>   | Crypto_VerifyResultType   |
|                        | <b>Direction</b>  | OUT   |
|                        | <b>Comment</b>  | Contains the verification result.   |
|                        | <b>Variation</b>  | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID |   |

|  |  |
|--|--|
|  | CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |
|--|--|

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

](SRS\_CryptoStack\_00090)

### 8.5.2.8 CsmSignatureGenerate

[SWS\_Csm\_91058]

|                        |  |                            |   |
|------------------------|--|----------------------------|---|
| <b>Name</b>            | CsmSignatureGenerate                                       |                            |   |
| <b>Comment</b>         | Asynchronous processing interface to generate a signature. |                            |   |
| <b>IsService</b>       | true   |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}           |                            |   |
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10   | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 12   | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|                        | 13   | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                        |   |   |
|------------------------|---|---|
| <b>Operation</b>       | SignatureGenerate   |   |
| <b>Comment</b>         | Operation to generate a signature.  |   |
| <b>Variation</b>       | --  |   |
| <b>Parameters</b>      | dataBuffer  |   |
|                        | <b>Type</b>   | Csm_DataPtr   |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | References the data from which the signature shall be generated.                      |
|                        | <b>Variation</b>  | --  |
|                        | dataLength  |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data from which the signature shall be generated. |
|                        | <b>Variation</b>  | --  |
|                        | resultBuffer  |   |
|                        | <b>Type</b>   | Csm_DataPtr   |
|                        | <b>Direction</b>  | OUT   |
|                        | <b>Comment</b>  | References the signature.   |
|                        | <b>Variation</b>  | --  |
|                        | resultLength  |   |
| <b>Type</b>            | uint32  |   |
| <b>Direction</b>       | INOUT   |   |
| <b>Comment</b>         | Contains the length in bytes of the signature.  |   |
| <b>Variation</b>       | --  |   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |   |

](SRS\_CryptoStack\_00090)

### 8.5.2.9 CsmSignatureVerify

[SWS\_Csm\_91059][



|                        |  |                            |   |
|------------------------|--|----------------------------|---|
| <b>Name</b>            | CsmSignatureVerify   |                            |   |
| <b>Comment</b>         | Asynchronous processing interface to execute the signature verification. |                            |   |
| <b>IsService</b>       | true   |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}                         |                            |   |
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10   | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 12   | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|                        | 13   | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                   |                                  |  |
|-------------------|----------------------------------|--|
| <b>Operation</b>  | SignatureVerify                  |  |
| <b>Comment</b>    | Operation to verify a signature. |  |
| <b>Variation</b>  | --                               |  |
| <b>Parameters</b> | dataBuffer                       |  |
|                   | <b>Type</b>                      | Csm_DataPtr  |
|                   | <b>Direction</b>                 | IN   |
|                   | <b>Comment</b>                   | References the data for which signature shall be verified. |
|                   | <b>Variation</b>                 | --   |
|                   | dataLength                       |  |
|                   | <b>Type</b>                      | uint32   |
|                   | <b>Direction</b>                 | IN   |

|                        |   |   |
|------------------------|---|---|
|                        | <b>Comment</b>  | Contains the length in bytes of the data for which signature shall be verified. |
|                        | <b>Variation</b>  | --  |
|                        | compareBuffer   |   |
|                        | <b>Type</b>   | Csm_DataPtr   |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | References the signature to be verified.  |
|                        | <b>Variation</b>  | --  |
|                        | compareLength   |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the length in bytes of the signature to be verified.                   |
|                        | <b>Variation</b>  | --  |
|                        | resultBuffer  |   |
|                        | <b>Type</b>   | Crypto_VerifyResultType   |
|                        | <b>Direction</b>  | OUT   |
| <b>Comment</b>         | Contains the verification result.   |   |
| <b>Variation</b>       | --  |   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY |   |

](SRS\_CryptoStack\_00090)

### 8.5.2.10 CsmRandomGenerate

[SWS\_Csm\_91060]

|                  |  |                      |
|------------------|--|----------------------|
| <b>Name</b>      | CsmRandomGenerate  |                      |
| <b>Comment</b>   | Asynchronous processing interface to execute the random number generation. |                      |
| <b>IsService</b> | true   |                      |
| <b>Variation</b> | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}                           |                      |
| <b>Possible</b>  | 0  | E_OK                 |
|                  |  | Operation successful |

|               |    |                            |  |
|---------------|----|----------------------------|--|
| <b>Errors</b> | 1  | E_NOT_OK                   | Operation failed   |
|               | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.                           |
|               | 4  | CRYPTO_E_ENTROPY_EXHAUSTED | Request failed, entropy of random number generator is exhausted. |
|               | 12 | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.                |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                        |   |  |
|------------------------|---|--|
| <b>Operation</b>       | RandomGenerate  |  |
| <b>Comment</b>         | Generates a random number and stores it in the memory location pointed by the resultBuffer pointer. |  |
| <b>Variation</b>       | --  |  |
| <b>Parameters</b>      | resultBuffer  |  |
|                        | <b>Type</b>   | Csm_DataPtr  |
|                        | <b>Direction</b>  | OUT  |
|                        | <b>Comment</b>  | References the random number.                              |
|                        | <b>Variation</b>  | --   |
|                        | resultLength  |  |
|                        | <b>Type</b>   | uint32   |
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Contains the length in bytes of the data of random number. |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_ENTROPY_EXHAUSTED                                     |  |

](SRS\_CryptoStack\_00090)

### 8.5.3 Client-Server-Interfaces (Key Management)

#### 8.5.3.1 CsmJobKeySetValid

[SWS\_Csm\_91035]

|                        |  |                       |   |
|------------------------|--|-----------------------|---|
| <b>Name</b>            | CsmJobKeySetValid                                |                       |   |
| <b>Comment</b>         | Interface to set a key valid.                    |                       |   |
| <b>IsService</b>       | true   |                       |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)} |                       |   |
| <b>Possible Errors</b> | 0  | E_OK                  | Operation successful                              |
|                        | 1  | E_NOT_OK              | Operation failed                                  |
|                        | 2  | CRYPTO_E_BUSY         | Request failed, service is still busy.            |
|                        | 12   | CRYPTO_E_JOB_CANCELED | Request failed because the job has been canceled. |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                        |                                   |                        |
|------------------------|-----------------------------------|------------------------|
| <b>Operation</b>       | KeySetValid                       |                        |
| <b>Comment</b>         | Operation to set a key valid.     |                        |
| <b>Variation</b>       | --                                |                        |
| <b>Parameters</b>      | key                               |                        |
|                        | <b>Type</b>                       | uint32                 |
|                        | <b>Direction</b>                  | IN                     |
|                        | <b>Comment</b>                    | Identifier of the key. |
|                        | <b>Variation</b>                  | --                     |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY |                        |

l()

### 8.5.3.2 CsmJobRandomSeed

#### [SWS\_Csm\_91036]

|                        |  |                        |   |
|------------------------|--|------------------------|---|
| <b>Name</b>            | CsmJobRandomSeed                                 |                        |   |
| <b>Comment</b>         | Interface to random seed operation.              |                        |   |
| <b>IsService</b>       | true   |                        |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)} |                        |   |
| <b>Possible Errors</b> | 0  | E_OK                   | Operation successful                              |
|                        | 1  | E_NOT_OK               | Operation failed                                  |
|                        | 2  | CRYPTO_E_BUSY          | Request failed, service is still busy.            |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID | Request failed, the key is not valid.             |
|                        | 12   | CRYPTO_E_JOB_CANCELED  | Request failed because the job has been canceled. |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                   |                                  |  |
|-------------------|----------------------------------|--|
| <b>Operation</b>  | RandomSeed                       |  |
| <b>Comment</b>    | Utilize the random seed service. |  |
| <b>Variation</b>  | --                               |  |
| <b>Parameters</b> | key                              |  |
|                   | <b>Type</b>                      | uint32   |
|                   | <b>Direction</b>                 | IN   |
|                   | <b>Comment</b>                   | Identifier of the key.   |
|                   | <b>Variation</b>                 | --   |
|                   | seedPtr                          |  |
|                   | <b>Type</b>                      | Csm_DataPtr  |
|                   | <b>Direction</b>                 | IN   |
|                   | <b>Comment</b>                   | Holds the data which shall be used for the random seed initialization. |
|                   | <b>Variation</b>                 | --   |

|                        |   |   |
|------------------------|---|---|
|                        | seedLength  |   |
|                        | <b>Type</b>   | uint32                                    |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the length of the seed in bytes. |
|                        | <b>Variation</b>  | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID |   |

]()

### 8.5.3.3 CsmJobKeyGenerate

[SWS\_Csm\_91037]

|                        |  |                        |   |
|------------------------|--|------------------------|---|
| <b>Name</b>            | CsmJobKeyGenerate                                |                        |   |
| <b>Comment</b>         | Interface to execute key generation.             |                        |   |
| <b>IsService</b>       | true   |                        |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)} |                        |   |
| <b>Possible Errors</b> | 0  | E_OK                   | Operation successful  |
|                        | 1  | E_NOT_OK               | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY          | Request failed, service is still busy.                                  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID | Request failed, the key is not valid.                                   |
|                        | 12   | CRYPTO_E_JOB_CANCELED  | Request failed because the job has been canceled.                       |
|                        | 13   | CRYPTO_E_KEY_EMPTY     | The service request failed because of uninitialized source key element. |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                  |  |
|------------------|--|
| <b>Operation</b> | KeyGenerate  |
| <b>Comment</b>   | Generates new key material and stores it in the key identified by keyId. |

|                        |   |                        |
|------------------------|---|------------------------|
| <b>Variation</b>       | --  |                        |
| <b>Parameters</b>      | key   |                        |
|                        | <b>Type</b>   | uint32                 |
|                        | <b>Direction</b>  | IN                     |
|                        | <b>Comment</b>  | Identifier of the key. |
|                        | <b>Variation</b>  | --                     |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_EMPTY |                        |

]()

### 8.5.3.4 CsmJobKeyDerive

[SWS\_Csm\_91038]

|                        |  |                            |   |
|------------------------|--|----------------------------|---|
| <b>Name</b>            | CsmJobKeyDerive                                  |                            |   |
| <b>Comment</b>         | Interface to execute key derive.                 |                            |   |
| <b>IsService</b>       | true   |                            |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)} |                            |   |
| <b>Possible Errors</b> | 0  | E_OK                       | Operation successful  |
|                        | 1  | E_NOT_OK                   | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY              | Request failed, service is still busy.  |
|                        | 6  | CRYPTO_E_KEY_READ_FAIL     | The service request failed because read access was denied.  |
|                        | 7  | CRYPTO_E_KEY_WRITE_FAIL    | The service request failed because write access was denied.   |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID     | Request failed, the key is not valid.   |
|                        | 10   | CRYPTO_E_KEY_SIZE_MISMATCH | Request failed because the key element is not partially accessible and the provided key element length is too short or too long for that key element. |
|                        | 12   | CRYPTO_E_JOB_CANCELED      | Request failed because the job has been canceled.   |
|                        | 13   | CRYPTO_E_KEY_EMPTY         | The service request failed because of uninitialized source key element.   |

|                  |           |
|------------------|-----------|
| <b>Operation</b> | CancelJob |
|------------------|-----------|

|                        |   |
|------------------------|---|
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                        |   |   |
|------------------------|---|---|
| <b>Operation</b>       | KeyDerive   |   |
| <b>Comment</b>         | Derives a new key by using the key elements in the given key. The given key contains the key elements for the password and salt. The derived key is stored in the key element with the id 1 of the key identified by targetCryptoKeyld. |   |
| <b>Variation</b>       | --  |   |
| <b>Parameters</b>      | key   |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Identifier of the key.  |
|                        | <b>Variation</b>  | --  |
|                        | targetKeyld   |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Holds the identifier of the key which is used to store the derived key. |
|                        | <b>Variation</b>  | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_READ_FAIL<br>CRYPTO_E_KEY_WRITE_FAIL<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_SIZE_MISMATCH<br>CRYPTO_E_KEY_EMPTY  |   |

]()

### 8.5.3.5 CsmJobKeyExchangeCalcPubVal

[SWS\_Csm\_91039]

|                  |  |
|------------------|--|
| <b>Name</b>      | CsmJobKeyExchangeCalcPubVal  |
| <b>Comment</b>   | Interface to execute calculation of the public value for key exchange. |
| <b>IsService</b> | true   |



|                        |  |                        |   |
|------------------------|--|------------------------|---|
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)} |                        |   |
| <b>Possible Errors</b> | 0  | E_OK                   | Operation successful  |
|                        | 1  | E_NOT_OK               | Operation failed  |
|                        | 2  | CRYPTO_E_BUSY          | Request failed, service is still busy.                                  |
|                        | 9  | CRYPTO_E_KEY_NOT_VALID | Request failed, the key is not valid.                                   |
|                        | 12   | CRYPTO_E_JOB_CANCELED  | Request failed because the job has been canceled.                       |
|                        | 13   | CRYPTO_E_KEY_EMPTY     | The service request failed because of uninitialized source key element. |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                      |  |   |
|----------------------|--|---|
| <b>Operation</b>     | KeyExchangeCalcPubVal  |   |
| <b>Comment</b>       | Calculates the public value of the current user for the key exchange and stores the public key in the provided buffer. |   |
| <b>Variation</b>     | --   |   |
| <b>Parameters</b>    | key  |   |
|                      | <b>Type</b>  | uint32  |
|                      | <b>Direction</b>   | IN  |
|                      | <b>Comment</b>   | Identifier of the key.  |
|                      | <b>Variation</b>   | --  |
|                      | publicValuePtr   |   |
|                      | <b>Type</b>  | Csm_KeyDataType_{Crypto}  |
|                      | <b>Direction</b>   | OUT   |
|                      | <b>Comment</b>   | Contains the pointer to the memory location where the public value shall be stored. |
|                      | <b>Variation</b>   | --  |
| publicValueLengthPtr |  |   |
| <b>Type</b>          | uint32   |   |

|                        |   |  |
|------------------------|---|--|
|                        | <b>Direction</b>  | INOUT  |
|                        | <b>Comment</b>  | Holds a pointer to the memory location in which the public value length in bytes is stored. On calling this function, this parameter shall contain the size of the buffer in bytes provided by publicValuePtr. When the request has finished, the actual length of the returned value shall be stored. |
|                        | <b>Variation</b>  | --   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_EMPTY |  |

l()

### 8.5.3.6 CsmJobKeyExchangeCalcSecret

[SWS\_Csm\_91040]

|                        |   |                        |   |
|------------------------|---|------------------------|---|
| <b>Name</b>            | CsmJobKeyExchangeCalcSecret   |                        |   |
| <b>Comment</b>         | Interface to execute calculation of shared secret for key exchange. |                        |   |
| <b>IsService</b>       | true  |                        |   |
| <b>Variation</b>       | Primitive = {ecuc(Csm/CsmPrimitives.SHORT-NAME)}                    |                        |   |
| <b>Possible Errors</b> | 0   | E_OK                   | Operation successful  |
|                        | 1   | E_NOT_OK               | Operation failed  |
|                        | 2   | CRYPTO_E_BUSY          | Request failed, service is still busy.                                  |
|                        | 9   | CRYPTO_E_KEY_NOT_VALID | Request failed, the key is not valid.                                   |
|                        | 12  | CRYPTO_E_JOB_CANCELED  | Request failed because the job has been canceled.                       |
|                        | 13  | CRYPTO_E_KEY_EMPTY     | The service request failed because of uninitialized source key element. |

|                        |   |
|------------------------|---|
| <b>Operation</b>       | CancelJob                                 |
| <b>Comment</b>         | Cancels the job.                          |
| <b>Variation</b>       | --  |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_JOB_CANCELED |

|                  |  |
|------------------|--|
| <b>Operation</b> | KeyExchangeCalcSecret  |
| <b>Comment</b>   | Calculates the shared secret key for the key exchange with the key material of the |

|                        |   |   |
|------------------------|---|---|
|                        | key identified by the keyId and the partner public key. The shared secret key is stored as a key element in the same key. |   |
| <b>Variation</b>       | --  |   |
| <b>Parameters</b>      | key   |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Identifier of the key.  |
|                        | <b>Variation</b>  | --  |
|                        | partnerPublicValuePtr   |   |
|                        | <b>Type</b>   | Csm_KeyDataType_{Crypto}  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Holds the pointer to the memory location containing the partner's public value. |
|                        | <b>Variation</b>  | --  |
|                        | partnerPublicValueLength  |   |
|                        | <b>Type</b>   | uint32  |
|                        | <b>Direction</b>  | IN  |
|                        | <b>Comment</b>  | Contains the number of bytes of the partner public value.                       |
| <b>Variation</b>       | --  |   |
| <b>Possible Errors</b> | E_OK<br>E_NOT_OK<br>CRYPTO_E_BUSY<br>CRYPTO_E_KEY_NOT_VALID<br>CRYPTO_E_KEY_EMPTY   |   |

l()

### 8.5.3.7 CallbackNotification

[SWS\_Csm\_00928]

|                        |  |    |    |
|------------------------|--|----|----|
| <b>Name</b>            | CallbackNotification                     |    |    |
| <b>Comment</b>         | Interface for the callback notification. |    |    |
| <b>IsService</b>       | true                                     |    |    |
| <b>Variation</b>       | --                                       |    |    |
| <b>Possible Errors</b> | --                                       | -- | -- |

|                        |   |  |
|------------------------|---|--|
| <b>Operation</b>       | CallbackNotification  |  |
| <b>Comment</b>         | Notifies the application with a return value that the job has finished. |  |
| <b>Variation</b>       | --  |  |
| <b>Parameters</b>      | result  |  |
|                        | <b>Type</b>   | Crypto_ResultType                                      |
|                        | <b>Direction</b>  | IN   |
|                        | <b>Comment</b>  | Return value that shall be returned to the application |
|                        | <b>Variation</b>  | --   |
| <b>Possible Errors</b> | --  |  |

](SRS\_CryptoStack\_00090)

## 8.5.4 Implementation Data Types

### 8.5.4.1 Crypto\_OperationModeType

[SWS\_Csm\_01029]

|                      |   |      |  |
|----------------------|---|------|--|
| <b>Name</b>          | Crypto_OperationModeType  |      |  |
| <b>Kind</b>          | Enumeration   |      |  |
| <b>Range</b>         | 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_UPDATE   | 0x02 | Operation Mode is "Update". Used to calculate intermediate results.  |
|                      | CRYPTO_OPERATIONMODE_STREAMSTART  | 0x03 | Operation Mode is "Stream Start". Mixture of "Start" and "Update". Used for streaming.   |
|                      | CRYPTO_OPERATIONMODE_FINISH   | 0x04 | Operation Mode is "Finish". The calculations shall be finalized.   |
|                      | CRYPTO_OPERATIONMODE_SINGLECALL   | 0x07 | Operation Mode is "Single Call". Mixture of "Start", "Update" and "Finish".  |
| <b>Description</b>   | 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". |      |  |
| <b>Variation</b>     | --  |      |  |
| <b>Available via</b> | Rte_Csm_Type.h  |      |  |

]()

#### 8.5.4.2 Crypto\_VerifyResultType

[SWS\_Csm\_01024]

|                      |  |      |  |
|----------------------|--|------|--|
| <b>Name</b>          | Crypto_VerifyResultType                                    |      |  |
| <b>Kind</b>          | Enumeration  |      |  |
| <b>Range</b>         | CRYPTO_E_VER_OK  | 0x00 | The result of the verification is "true", i.e. the two compared elements are identical. This return code shall be given as value "0"       |
|                      | CRYPTO_E_VER_NOT_OK  | 0x01 | The result of the verification is "false", i.e. the two compared elements are not identical. This return code shall be given as value "1". |
| <b>Description</b>   | Enumeration of the result type of verification operations. |      |  |
| <b>Variation</b>     | --   |      |  |
| <b>Available via</b> | Rte_Csm_Type.h   |      |  |

]()

#### 8.5.4.3 Csm\_DataPtr

[SWS\_Csm\_91061]

|                      |   |
|----------------------|---|
| <b>Name</b>          | Csm_DataPtr                               |
| <b>Kind</b>          | Const Pointer                             |
| <b>Type</b>          | const uint8*                              |
| <b>Description</b>   | Byte-pointer to the input or output data. |
| <b>Variation</b>     | --  |
| <b>Available via</b> | Rte_Csm_Type.h                            |

](SRS\_CryptoStack\_00090)

#### 8.5.4.4 Csm\_KeyDataType\_{Crypto}

[SWS\_Csm\_00828]

|             |  |                     |       |
|-------------|--|---------------------|-------|
| <b>Name</b> | Csm_KeyDataType_{Crypto}   |                     |       |
| <b>Kind</b> | Array  | <b>Element type</b> | uint8 |
| <b>Size</b> | max({ecuc(Csm/CsmKeys/CsmKey/CsmKeyRef->CryIfKey/CryIfKeyRef->CryptoKey/CryptoKeyTypeRef->CryptoKeyType/CryptoKeyElementRef->CryptoKeyElement/CryptoKeyElementSize) Elements |                     |       |

|                      |  |
|----------------------|--|
| <b>Description</b>   | Array long enough to store any key element of the considered key |
| <b>Variation</b>     | Crypto = {ecuc(Csm/CsmKeys/CsmKey.SHORT-NAME)}                   |
| <b>Available via</b> | Rte_Csm_Type.h   |

I()

#### 8.5.4.5 Csm\_ResultType

[SWS\_Csm\_91001]{OBSOLETE} [

|                      |  |      |   |
|----------------------|--|------|---|
| <b>Name</b>          | Csm_ResultType (obsolete)  |      |   |
| <b>Kind</b>          | Type   |      |   |
| <b>Derived from</b>  | Std_ReturnType   |      |   |
| <b>Range</b>         | E_OK   | 0x00 | The service request is successful.  |
|                      | E_NOT_OK   | 0x01 | The service request failed.   |
|                      | E_ENTROPY_EXHAUSTED  | 0x03 | The service request failed because the entropy of random number generator is exhausted. |
|                      | E_KEY_READ_FAIL  | 0x04 | The service request failed because read access was denied.                              |
|                      | E_KEY_NOT_AVAILABLE  | 0x05 | The service request failed because the key is not available.                            |
|                      | E_KEY_NOT_VALID  | 0x06 | The service request failed because key was not valid.                                   |
|                      | E_JOB_CANCELED   | 0x07 | The service request failed because the job was canceled                                 |
|                      | E_KEY_EMPTY  | 0x08 | The service request failed because of uninitialized source key element.                 |
| <b>Description</b>   | Csm module specific return values for use in Std_ReturnType that could occur on async.<br><b>Tags:</b> atp.Status=obsolete |      |   |
| <b>Available via</b> | Rte_Csm_Type.h   |      |   |

](SRS\_CryptoStack\_00095)

#### 8.5.4.6 Crypto\_ResultType

[SWS\_Csm\_91044][

|             |                   |
|-------------|-------------------|
| <b>Name</b> | Crypto_ResultType |
| <b>Kind</b> | Enumeration       |

|                      |  |      |  |
|----------------------|--|------|--|
| <b>Range</b>         | E_OK                                       | 0x00 | The service request is successful.   |
|                      | E_NOT_OK                                   | 0x01 | The service request failed.  |
|                      | CRYPTO_E_BUSY                              | 0x02 | The service request failed because the service is still busy                               |
|                      | CRYPTO_E_ENTROPY_EXHAUSTED                 | 0x04 | The service request failed because the entropy of the random number generator is exhausted |
|                      | CRYPTO_E_KEY_READ_FAIL                     | 0x06 | The service request failed because read access was denied                                  |
|                      | CRYPTO_E_KEY_WRITE_FAIL                    | 0x07 | The service request failed because the writing access failed                               |
|                      | CRYPTO_E_KEY_NOT_AVAILABLE                 | 0x08 | The service request failed because the key is not available                                |
|                      | CRYPTO_E_KEY_NOT_VALID                     | 0x09 | The service request failed because the key is invalid.                                     |
|                      | CRYPTO_E_KEY_SIZE_MISMATCH                 | 0x0A | The service request failed because the key size does not match.                            |
|                      | CRYPTO_E_JOB_CANCELED                      | 0x0C | The service request failed because the Job has been canceled.                              |
|                      | CRYPTO_E_KEY_EMPTY                         | 0x0D | The service request failed because of uninitialized source key element.                    |
| <b>Description</b>   | Return for Std_ReturnType for Cryptostack. |      |  |
| <b>Variation</b>     | --   |      |  |
| <b>Available via</b> | Rte_Csm_Type.h                             |      |  |

](SRS\_CryptoStack\_00095)

#### 8.5.4.7 Csm\_HashDataType\_{Crypto}

[SWS\_Csm\_01920][

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_HashDataType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmHash/CsmHashConfig/CsmHashDataMaxLength) Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data which shall be hashed.                   |                     |       |
| <b>Variation</b>     | Crypto={ecuc/Csm/CsmPrimitives.SHORT-NAME}                                   |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.8 Csm\_HashResultType\_{Crypto}

##### [SWS\_Csm\_00912]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_HashResultType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmHash/CsmHashConfig/CsmHashResultLength)} Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data of the hash.                             |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}                                  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.9 Csm\_MacGenerateDataType\_{Crypto}

##### [SWS\_Csm\_00935]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_MacGenerateDataType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig/CsmMacGenerateDataMaxLength)} Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data from which a MAC shall be generated.                           |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.10 Csm\_MacGenerateResultType\_{Crypto}

##### [SWS\_Csm\_00927]

|                      |   |                     |       |
|----------------------|---|---------------------|-------|
| <b>Name</b>          | Csm_MacGenerateResultType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array   | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmMacGenerate/CsmMacGenerateConfig/CsmMacGenerateResultLength)} Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data of the MAC.   |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h  |                     |       |



](SRS\_CryptoStack\_00090)

#### 8.5.4.11 Csm\_MacVerifyDataType\_{Crypto}

[SWS\_Csm\_00802][

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_MacVerifyDataType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerifyConfig/CsmMacVerifyData MaxLength) Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data for whichs MAC shall be verified.                        |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.12 Csm\_MacVerifyCompareType\_{Crypto}

[SWS\_Csm\_00803][

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_MacVerifyCompareType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmMacVerify/CsmMacVerifyConfig/CsmMacVerify CompareLength)/8 Elements |                     |       |
| <b>Description</b>   | Array long enough to store a MAC to be verified.   |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.13 Csm\_EncryptDataType\_{Crypto}

[SWS\_Csm\_01921][

|                    |  |                     |       |
|--------------------|--|---------------------|-------|
| <b>Name</b>        | Csm_EncryptDataType_{Crypto}   |                     |       |
| <b>Kind</b>        | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>        | {ecuc(Csm/CsmPrimitives/CsmEncrypt/CsmEncryptConfig/CsmEncryptDataMax Length) Elements |                     |       |
| <b>Description</b> | Array long enough to store the data to be encrypted.                                   |                     |       |
| <b>Variation</b>   | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |

|                      |                |
|----------------------|----------------|
| <b>Available via</b> | Rte_Csm_Type.h |
|----------------------|----------------|

](SRS\_CryptoStack\_00090)

#### 8.5.4.14 Csm\_EncryptResultType\_{Crypto}

[SWS\_Csm\_01922]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_EncryptResultType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmEncrypt/CsmEncryptConfig/CsmEncryptResultMaxLength) Elements} |                     |       |
| <b>Description</b>   | Array long enough to store the data of the cipher.                                       |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.15 Csm\_DecryptDataType\_{Crypto}

[SWS\_Csm\_01923]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_DecryptDataType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmDecrypt/CsmDecryptConfig/CsmDecryptDataMaxLength) Elements} |                     |       |
| <b>Description</b>   | Array long enough to store the data to be decrypted.                                   |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.16 Csm\_DecryptResultType\_{Crypto}

[SWS\_Csm\_01924]

|             |  |                     |       |
|-------------|--|---------------------|-------|
| <b>Name</b> | Csm_DecryptResultType_{Crypto}   |                     |       |
| <b>Kind</b> | Array  | <b>Element type</b> | uint8 |
| <b>Size</b> | {ecuc(Csm/CsmPrimitives/CsmDecrypt/CsmDecryptConfig/CsmDecryptResultMaxLength) Elements} |                     |       |

|                      |   |
|----------------------|---|
| <b>Description</b>   | Array long enough to store the data of the decrypted plaintext. |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}                     |
| <b>Available via</b> | Rte_Csm_Type.h  |

](SRS\_CryptoStack\_00090)

#### 8.5.4.17 Csm\_AEADEncryptPlaintextType\_{Crypto}

[SWS\_Csm\_01925]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_AEADEncryptPlaintextType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEADEncryptPlaintextMaxLength) Elements |                     |       |
| <b>Description</b>   | Array long enough to store the plaintext to be encrypted with AEAD.                                    |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.18 Csm\_AEADEncryptAssociatedDataType\_{Crypto}

[SWS\_Csm\_01928]

|                      |   |                     |       |
|----------------------|---|---------------------|-------|
| <b>Name</b>          | Csm_AEADEncryptAssociatedDataType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array   | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEADEncryptAssociatedDataMaxLength) Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data of the header.  |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h  |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.19 Csm\_AEADEncryptCiphertextType\_{Crypto}

[SWS\_Csm\_01927]

|             |  |                     |       |
|-------------|--|---------------------|-------|
| <b>Name</b> | Csm_AEADEncryptCiphertextType_{Crypto} |                     |       |
| <b>Kind</b> | Array                                  | <b>Element type</b> | uint8 |

|                      |  |
|----------------------|--|
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEADEncryptCiphertextMaxLength)} Elements |
| <b>Description</b>   | Array long enough to store the data of the cipher.   |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |
| <b>Available via</b> | Rte_Csm_Type.h   |

](SRS\_CryptoStack\_00090)

#### 8.5.4.20 Csm\_AEADEncryptTagType\_{Crypto}

[SWS\_Csm\_01926]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_AEADEncryptTagType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmAEADEncrypt/CsmAEADEncryptConfig/CsmAEADEncryptTagLength)} Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data of the Tag.  |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.21 Csm\_AEADDecryptCiphertextType\_{Crypto}

[SWS\_Csm\_00922]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_AEADDecryptCiphertextType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmAEADDecrypt/CsmAEADDecryptConfig/CsmAEADDecryptCiphertextMaxLength)} Elements |                     |       |
| <b>Description</b>   | Array long enough to store the ciphertext to be decrypted with AEAD.                       |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.22 Csm\_AEADDecryptAssociatedDataType\_{Crypto}

[SWS\_Csm\_00923]

|                      |   |                     |       |
|----------------------|---|---------------------|-------|
| <b>Name</b>          | Csm_AEADDecryptAssociatedDataType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array   | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmAEADDecrypt/CsmAEADDecryptConfig/CsmAEADDecryptAssociatedDataMaxLength) Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data of the header.  |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h  |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.23 Csm\_AEADDecryptTagType\_{Crypto}

[SWS\_Csm\_01074]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_AEADDecryptTagType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | (((ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/CsmAEADDecryptTagLength))+7)/8) Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data of the Tag.  |                     |       |
| <b>Variation</b>     | Crypto = {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.24 Csm\_AEADDecryptPlaintextType\_{Crypto}

[SWS\_Csm\_01075]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_AEADDecryptPlaintextType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmAEADDecrypt/CsmAEADDecryptConfig/CsmAEADDecryptPlaintextMaxLength) Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data of the plaintext.  |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.25 Csm\_SignatureGenerateDataType\_{Crypto}

##### [SWS\_Csm\_01083]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_SignatureGenerateDataType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmSignatureGenerate/CsmSignatureGenerateConfig/CsmSignatureGenerateDataMaxLength) Elements} |                     |       |
| <b>Description</b>   | Array long enough to store the data from which the signature shall be generated.                                     |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_01076)

#### 8.5.4.26 Csm\_SignatureGenerateResultType\_{Crypto}

##### [SWS\_Csm\_01077]

|                      |   |                     |       |
|----------------------|---|---------------------|-------|
| <b>Name</b>          | Csm_SignatureGenerateResultType_{Crypto}  |                     |       |
| <b>Kind</b>          | Array   | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmSignatureGenerate/CsmSignatureGenerateConfig/CsmSignatureGenerateResultLength) Elements} |                     |       |
| <b>Description</b>   | Array long enough to store the signature and its length.  |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h  |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.27 Csm\_SignatureVerifyDataType\_{Crypto}

##### [SWS\_Csm\_01078]

|                      |  |                     |       |
|----------------------|--|---------------------|-------|
| <b>Name</b>          | Csm_SignatureVerifyDataType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array  | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmSignatureVerify/CsmSignatureVerifyConfig/CsmSignatureVerifyDataMaxLength) Elements} |                     |       |
| <b>Description</b>   | Array long enough to store the data for whichs signature shall be verified.                                    |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}  |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h   |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.28 Csm\_SignatureVerifyCompareType\_{Crypto}

[SWS\_Csm\_01079]

|                      |   |                     |       |
|----------------------|---|---------------------|-------|
| <b>Name</b>          | Csm_SignatureVerifyCompareType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array   | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmSignatureVerify/CsmSignatureVerifyConfig/CsmSignatureVerifyCompareLength) Elements |                     |       |
| <b>Description</b>   | Array long enough to store a signature to be verified.  |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h  |                     |       |

](SRS\_CryptoStack\_00090)

#### 8.5.4.29 Csm\_RandomGenerateResultType\_{Crypto}

[SWS\_Csm\_00930]

|                      |   |                     |       |
|----------------------|---|---------------------|-------|
| <b>Name</b>          | Csm_RandomGenerateResultType_{Crypto}   |                     |       |
| <b>Kind</b>          | Array   | <b>Element type</b> | uint8 |
| <b>Size</b>          | {ecuc(Csm/CsmPrimitives/CsmRandomGenerate/CsmRandomGenerateConfig/CsmRandomGenerateResultLength) Elements |                     |       |
| <b>Description</b>   | Array long enough to store the data of the random number.   |                     |       |
| <b>Variation</b>     | Crypto= {ecuc/Csm/CsmPrimitives.SHORT-NAME}   |                     |       |
| <b>Available via</b> | Rte_Csm_Type.h  |                     |       |

](SRS\_CryptoStack\_00090)

### 8.5.5 Ports

#### 8.5.5.1 CsmKey\_{Key}

[SWS\_Csm\_01042]

|                    |   |                  |                        |
|--------------------|---|------------------|------------------------|
| <b>Name</b>        | CsmKey_{Key}  |                  |                        |
| <b>Kind</b>        | ProvidedPort  | <b>Interface</b> | CsmKeyManagement_{Key} |
| <b>Description</b> | Port related to a specific cryptographic key to execute the key management functions synchronously. |                  |                        |

|                                       |   |                                     |
|---------------------------------------|---|-------------------------------------|
| <b>Port Defined Argument Value(s)</b> | <b>Type</b>   | uint32                              |
|                                       | <b>Value</b>  | {ecuc(Csm/CsmKeys/CsmKey/CsmKeyId)} |
| <b>Variation</b>                      | {ecuc(Csm/CsmKeys/CsmKey.CsmKeyUsePort)} == TRUE<br>Key = {ecuc(Csm/CsmKeys/CsmKey.SHORT-NAME)} |                                     |

](SRS\_CryptoStack\_00090, SRS\_CryptoStack\_00091)

### 8.5.5.2 CsmJob\_{Job} (CRYPTO\_USE\_PORT)

[SWS\_Csm\_91023]

|                                       |   |                                     |    |
|---------------------------------------|---|-------------------------------------|----|
| <b>Name</b>                           | CsmJob_{Job}  |                                     |    |
| <b>Kind</b>                           | ProvidedPort  | <b>Interface</b>                    | -- |
| <b>Description</b>                    | Port related to a specific cryptographic job to execute the assigned cryptographic calculations synchronously.  |                                     |    |
| <b>Port Defined Argument Value(s)</b> | <b>Type</b>   | uint32                              |    |
|                                       | <b>Value</b>  | {ecuc(Csm/CsmJobs/CsmJob.CsmJobId)} |    |
|                                       | <b>Type</b>   | Crypto_OperationModeType            |    |
|                                       | <b>Value</b>  | CRYPTO_OPERATIONMODE_SINGLECALL     |    |
| <b>Variation</b>                      | ({ecuc(Csm/CsmJobs/CsmJob.CsmJobInterfaceUsePort)} == CRYPTO_USE_PORT) &&({ecuc(Csm/CsmJobs/CsmJob.CsmJobPrimitiveRef)} != NULL)<br>Job = {ecuc(Csm/CsmJobs/CsmJob.SHORT-NAME)}<br>Primitive = {ecuc(Csm/CsmJobs/CsmJob.CsmJobPrimitiveRef->CsmPrimitives/*.SHORT-NAME)}<br>PrimitiveCfg = {ecuc(Csm/CsmPrimitives/{Primitive}/{Primitive}Config.SHORT-NAME)} |                                     |    |

](SRS\_CryptoStack\_00090, SRS\_CryptoStack\_00091)

### 8.5.5.3 CsmJob\_{Job} (CRYPTO\_USE\_PORT\_OPTIMIZED)

[SWS\_Csm\_91062]

|                                       |   |                                     |    |
|---------------------------------------|---|-------------------------------------|----|
| <b>Name</b>                           | CsmJob_{Job}  |                                     |    |
| <b>Kind</b>                           | ProvidedPort  | <b>Interface</b>                    | -- |
| <b>Description</b>                    | Port related to a specific cryptographic job to execute the assigned cryptographic calculations asynchronously. |                                     |    |
| <b>Port Defined Argument Value(s)</b> | <b>Type</b>   | uint32                              |    |
|                                       | <b>Value</b>  | {ecuc(Csm/CsmJobs/CsmJob.CsmJobId)} |    |
|                                       | <b>Type</b>   | Crypto_OperationModeType            |    |



|                  |   |                                 |
|------------------|---|---------------------------------|
|                  | <b>Value</b>  | CRYPTO_OPERATIONMODE_SINGLECALL |
| <b>Variation</b> | ({{ecuc(Csm/CsmJobs/CsmJob.CsmJobInterfaceUsePort)}} == CRYPTO_USE_PORT_OPTIMIZED) &&({{ecuc(Csm/CsmJobs/CsmJob.CsmJobPrimitiveRef)}} != NULL)<br>Job = {{ecuc(Csm/CsmJobs/CsmJob.SHORT-NAME)}}<br>Primitive = {{ecuc(Csm/CsmJobs/CsmJob.CsmJobPrimitiveRef->CsmPrimitives/* .SHORT-NAME)}} |                                 |

](SRS\_CryptoStack\_00090, SRS\_CryptoStack\_00091)

#### 8.5.5.4 CallbackNotification\_{Job}

[SWS\_Csm\_00934]

|                    |  |                  |                      |
|--------------------|--|------------------|----------------------|
| <b>Name</b>        | CallbackNotification_{Job}   |                  |                      |
| <b>Kind</b>        | RequiredPort   | <b>Interface</b> | CallbackNotification |
| <b>Description</b> | Port for the callback notification.  |                  |                      |
| <b>Variation</b>   | ({{ecuc(Csm/CsmJobs/CsmJob.CsmProcessingMode)}}==CRYPTO_PROCESSING_ASYN)&&(CsmJob/CsmJobInterfaceUsePort!=CRYPTO_USE_FNC)<br>Job = {{ecuc(Csm/CsmJobs/CsmJob.SHORT-NAME)}} |                  |                      |

](SRS\_CryptoStack\_00090, SRS\_CryptoStack\_00091)

## 9 Sequence Diagrams

The following sequence diagrams concentrate on the interaction between the CSM module and software components respectively the ECU state manager.

### 9.1 Asynchronous Calls

The following diagram (Sequence diagram for asynchronous call) shows a sample sequence of function calls for a request performed asynchronously. The result of the asynchronous function can be accessed after an asynchronous notification (invocation of the configured callback function).

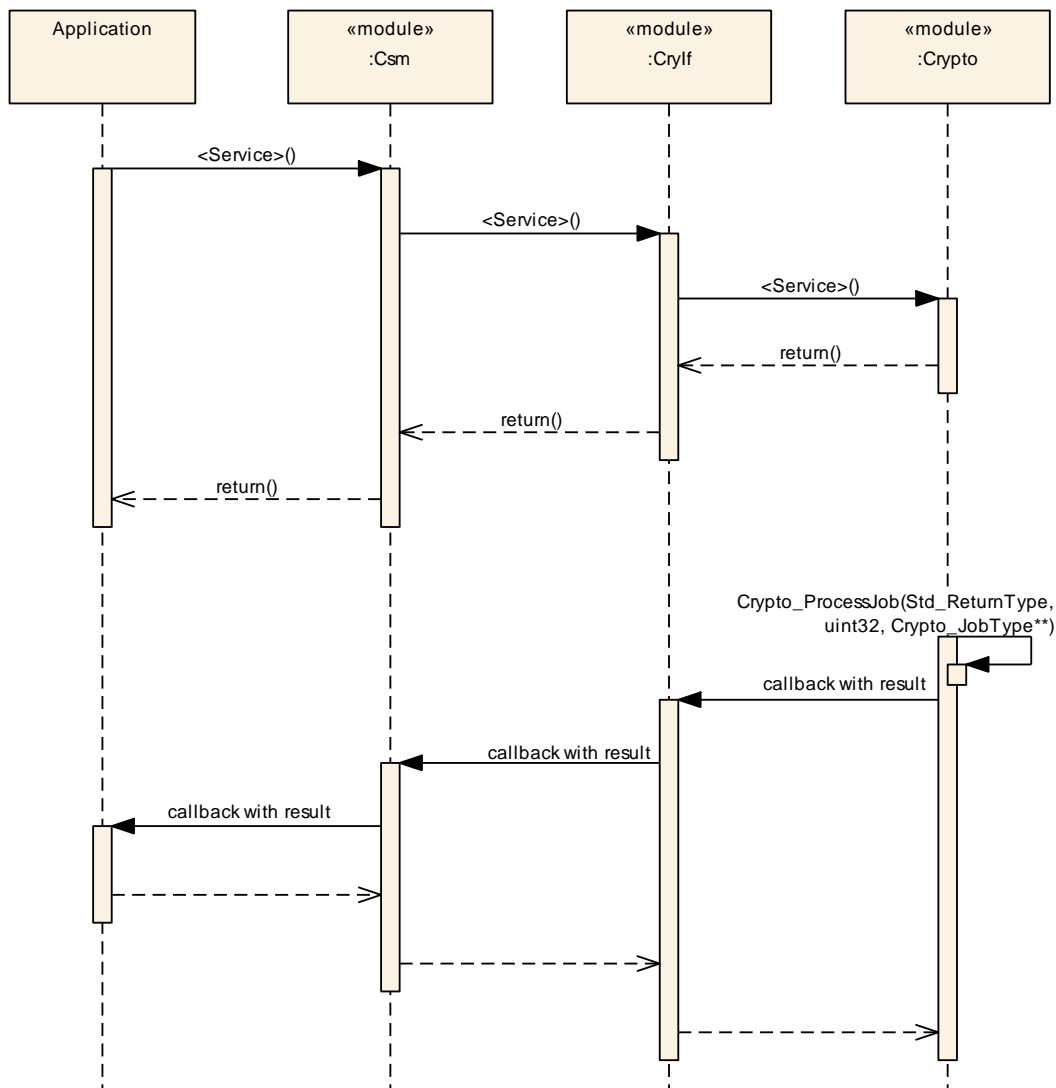


Figure 9-1 Sequence Diagram for Asynchronous Call with Callback

## 9.2 Synchronous Calls

The following diagram (Sequence diagram for synchronous calls) shows a sample sequence of function calls with the scheduler for a request performed synchronously.

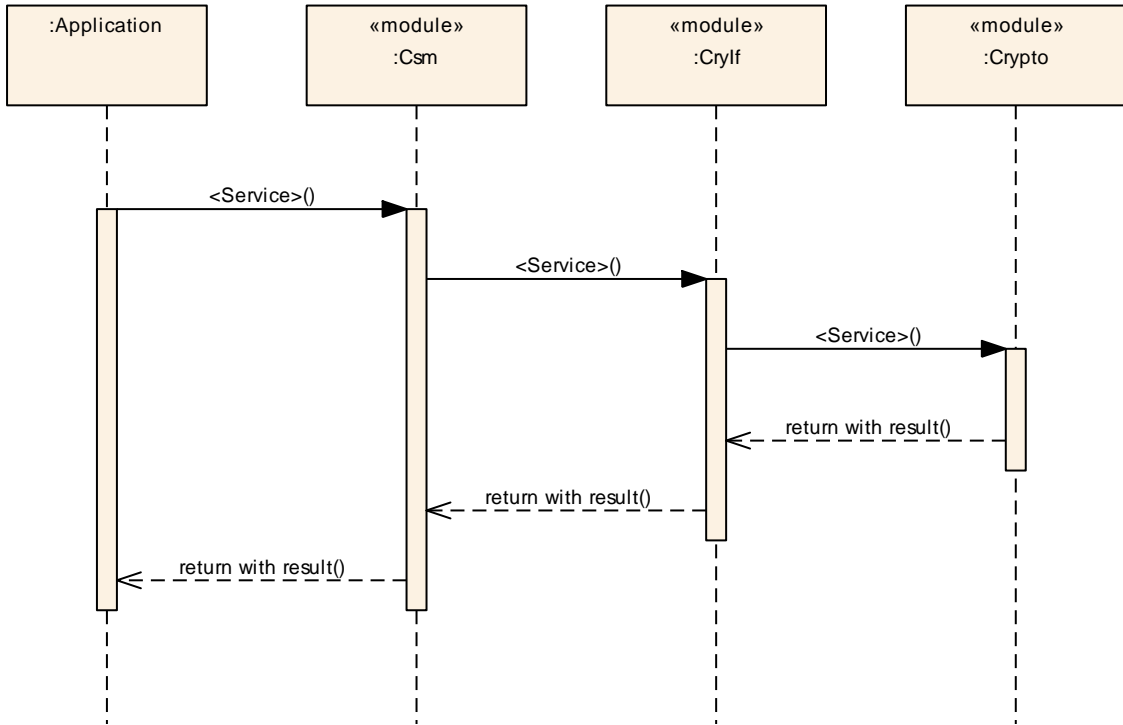


Figure 9-2 Sequence Diagram for Synchronous Call

## 10 Configuration

In general, this chapter defines configuration parameters and their clustering into containers. In order to support the specification Chapter 10.1 describes fundamentals. It also specifies a template (table) you shall use for the parameter specification.

Chapter 10.2 specifies the structure (containers) and the parameters of the module CSM.

Chapter 10.3 specifies published information of the module CSM.

### 10.1 How to Read this Chapter

For details refer to the chapter 10.1 “Introduction to configuration specification” in *SWS\_BSWGeneral*.

### 10.2 Containers and Configuration Parameters

The following chapters summarize all configuration parameters. The detailed meanings of the parameters describe Chapters 7 and Chapter 8.

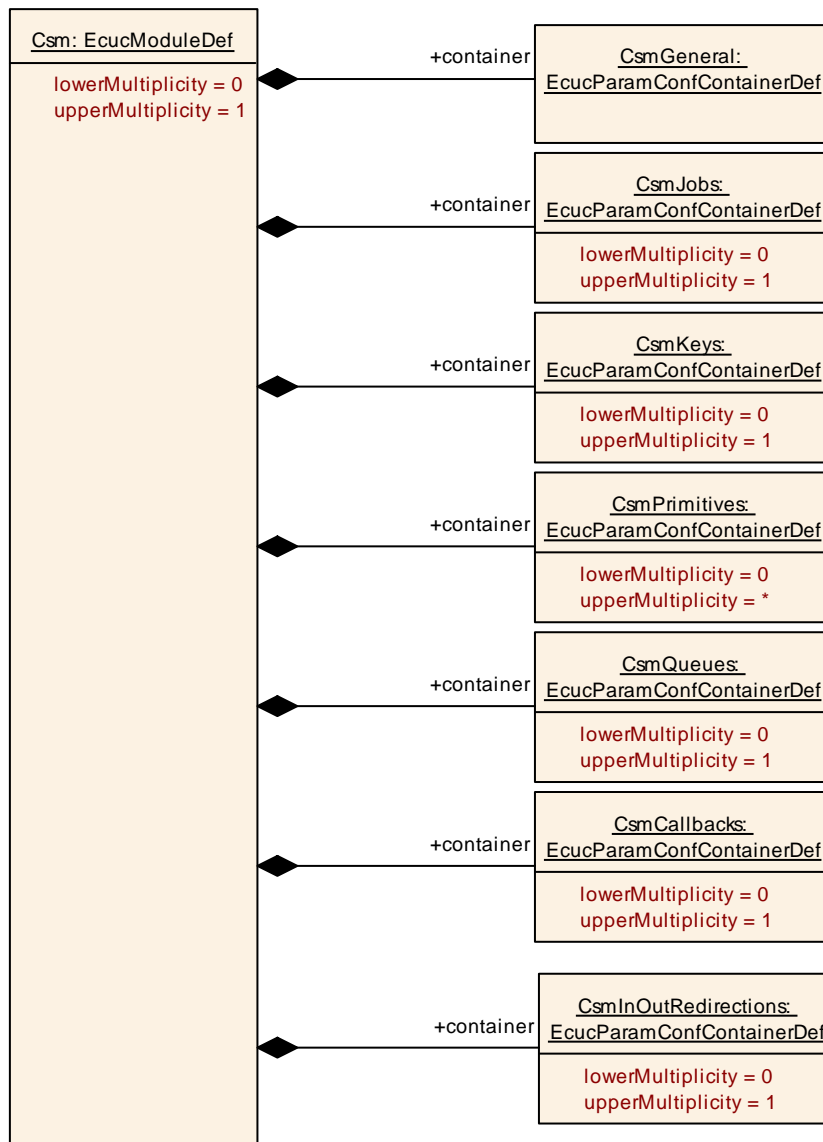


Figure 9-3 Crypto Service Manager Layout

### 10.2.1 Csm

|                                   |   |
|-----------------------------------|---|
| <b>SWS Item</b>                   | ECUC_Csm_00818 :  |
| <b>Module Name</b>                | Csm   |
| <b>Module Description</b>         | Configuration of the Csm (CryptoServiceManager) module. |
| <b>Post-Build Variant Support</b> | false   |
| <b>Supported Config Variants</b>  | VARIANT-PRE-COMPILE                                     |

| <b>Included Containers</b> |                     |  |
|----------------------------|---------------------|--|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                        |
| CsmCallbacks               | 0..1                | Container for callback function configurations   |
| CsmGeneral                 | 1                   | Container for common configuration options.      |
| CsmInOutRedirections       | 0..1                | Configuration for CSM redirection configurations |
| CsmJobs                    | 0..1                | Container for configuration of CSM jobs.         |
| CsmKeys                    | 0..1                | Container for CSM key configurations.            |
| CsmPrimitives              | 0..*                | Container for configuration of CsmPrimitives     |

|           |      |  |
|-----------|------|--|
| CsmQueues | 0..1 | Container for CSM queue configurations |
|-----------|------|--|

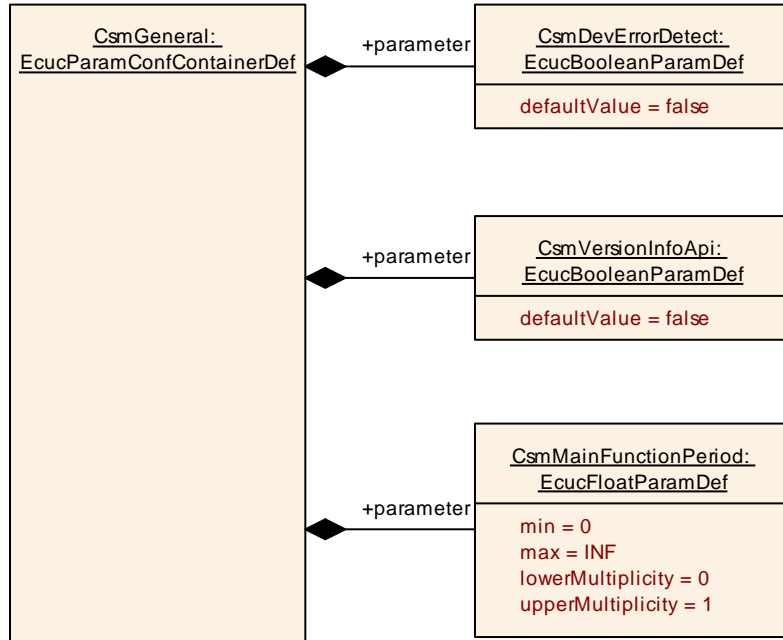


Figure 9-4 Crypto Service Manager General Layout

10.2.2 CsmGeneral

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | ECUC_Csm_00002 :                            |    |              |
| <b>Container Name</b>                   | CsmGeneral                                  |    |              |
| <b>Parent Container</b>                 | Csm   |    |              |
| <b>Description</b>                      | Container for common configuration options. |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|   | <b>Link time</b>                            | -- |              |
|   | <b>Post-build time</b>                      | -- |              |
| <b>Configuration Parameters</b>         |   |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | ECUC_Csm_00001 :  |    |              |
| <b>Name</b>                             | CsmDevErrorDetect   |    |              |
| <b>Parent Container</b>                 | CsmGeneral  |    |              |
| <b>Description</b>                      | Switches the development error detection and notification on or off. <ul style="list-style-type: none"> <li>• true: detection and notification is enabled.</li> <li>• false: detection and notification is disabled.</li> </ul> |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucBooleanParamDef   |    |              |
| <b>Default value</b>                    | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |

|                           |                        |    |  |
|---------------------------|------------------------|----|--|
|                           | <b>Link time</b>       | -- |  |
|                           | <b>Post-build time</b> | -- |  |
| <b>Scope / Dependency</b> | scope: local           |    |  |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00113 :</b>  |    |              |
| <b>Name</b>                             | CsmMainFunctionPeriod  |    |              |
| <b>Parent Container</b>                 | CsmGeneral   |    |              |
| <b>Description</b>                      | Specifies the period of main function Csm_MainFunction in seconds. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucFloatParamDef  |    |              |
| <b>Range</b>                            | ]0 .. INF[   |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00003 :</b>   |    |              |
| <b>Name</b>                             | CsmVersionInfoApi   |    |              |
| <b>Parent Container</b>                 | CsmGeneral  |    |              |
| <b>Description</b>                      | Pre-processor switch to enable and disable availability of the API Csm_GetVersionInfo().<br>True: API Csm_GetVersionInfo() is available.<br>False: API Csm_GetVersionInfo() is not available. |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucBooleanParamDef   |    |              |
| <b>Default value</b>                    | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

**No Included Containers**

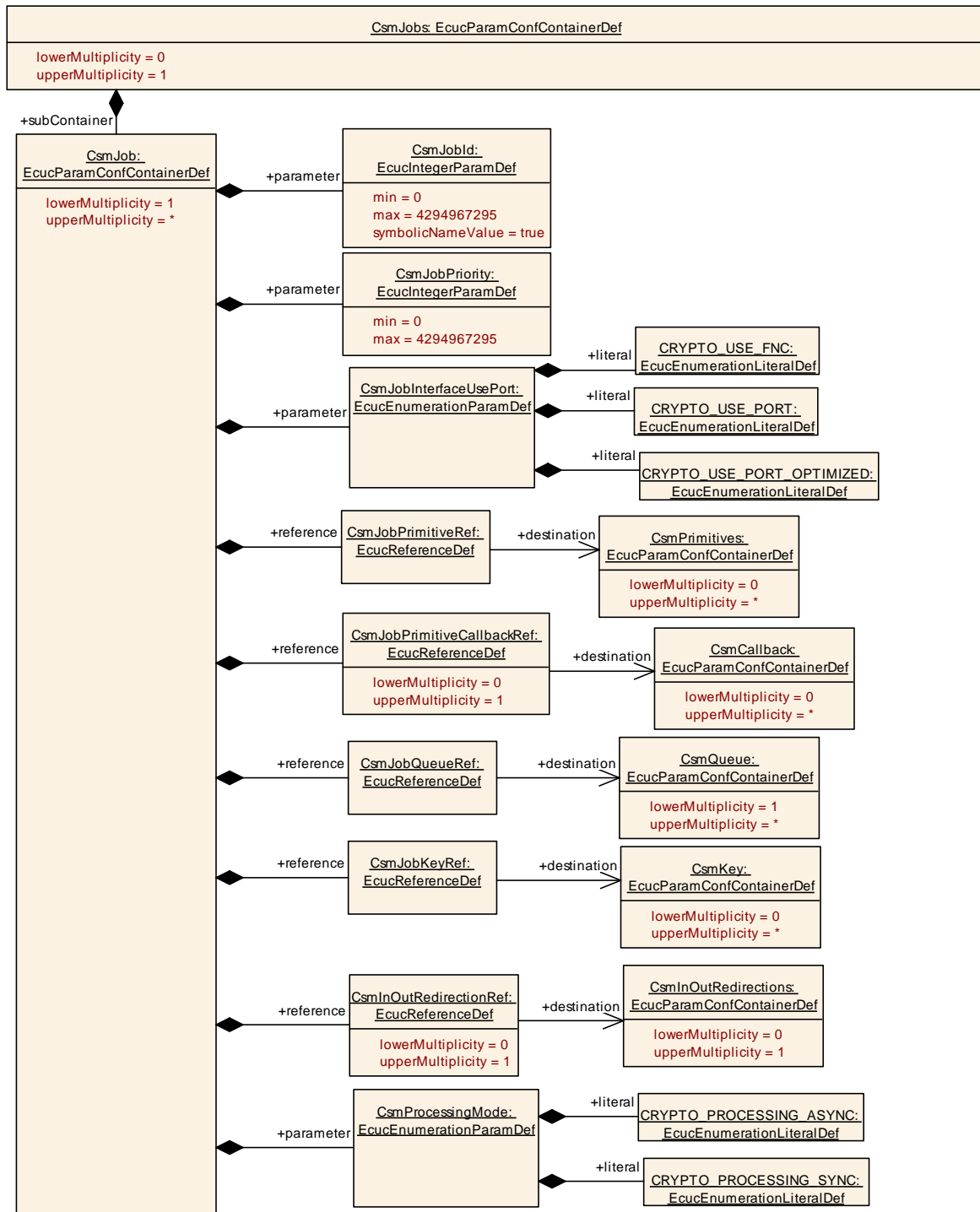


Figure 9-5 CsmJobs Layout

10.2.3 CsmJobs

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00112 :</b>                  |    |              |
| <b>Container Name</b>                   | CsmJobs                                  |    |              |
| <b>Parent Container</b>                 | Csm                                      |    |              |
| <b>Description</b>                      | Container for configuration of CSM jobs. |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                  | X  | All Variants |
|   | <b>Link time</b>                         | -- |              |



|                                 |                        |   |  |
|---------------------------------|------------------------|---|--|
|                                 | <b>Post-build time</b> | --  |  |
| <b>Configuration Parameters</b> |                        |   |  |
| <b>Included Containers</b>      |                        |   |  |
| <b>Container Name</b>           | <b>Multiplicity</b>    | <b>Scope / Dependency</b>   |  |
| CsmJob                          | 1..*                   | Container for configuration of CSM job. The container name serves as a symbolic name for the identifier of a job configuration. |  |

### 10.2.4 CsmJob

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00118 :</b>   |    |              |
| <b>Container Name</b>                   | CsmJob  |    |              |
| <b>Parent Container</b>                 | CsmJobs   |    |              |
| <b>Description</b>                      | Container for configuration of CSM job. The container name serves as a symbolic name for the identifier of a job configuration. |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Configuration Parameters</b>         |   |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00119 :</b>   |    |              |
| <b>Name</b>                             | CsmJobId  |    |              |
| <b>Parent Container</b>                 | CsmJob  |    |              |
| <b>Description</b>                      | Identifier of the CSM job. The set of actually configured identifiers shall be consecutive and gapless. |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef (Symbolic Name generated for this parameter)  |    |              |
| <b>Range</b>                            | 0 .. 4294967295   |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                                  |                                   |    |                         |
|----------------------------------|-----------------------------------|----|-------------------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00275 :</b>           |    |                         |
| <b>Name</b>                      | CsmJobInterfaceUsePort            |    |                         |
| <b>Parent Container</b>          | CsmJob                            |    |                         |
| <b>Description</b>               | Does the job need RTE interfaces? |    |                         |
| <b>Multiplicity</b>              | 1                                 |    |                         |
| <b>Type</b>                      | EcucEnumerationParamDef           |    |                         |
| <b>Range</b>                     | CRYPTO_USE_FNC                    |    | Port is not used.       |
|                                  | CRYPTO_USE_PORT                   |    | Port is used.           |
|                                  | CRYPTO_USE_PORT_OPTIMIZED         |    | DATA_REFERENCE is used. |
| <b>Post-Build Variant Value</b>  | false                             |    |                         |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>           | X  | All Variants            |
|                                  | <b>Link time</b>                  | -- |                         |
|                                  | <b>Post-build time</b>            | -- |                         |

|                           |              |
|---------------------------|--------------|
| <b>Scope / Dependency</b> | scope: local |
|---------------------------|--------------|

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00120 :</b>  |    |              |
| <b>Name</b>                             | CsmJobPriority   |    |              |
| <b>Parent Container</b>                 | CsmJob   |    |              |
| <b>Description</b>                      | Priority of the job.<br>The higher the value, the higher the job's priority. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef  |    |              |
| <b>Range</b>                            | 0 .. 4294967295  |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|                                  |  |    |              |
|----------------------------------|--|----|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00276 :</b>  |    |              |
| <b>Name</b>                      | CsmProcessingMode  |    |              |
| <b>Parent Container</b>          | CsmJob   |    |              |
| <b>Description</b>               | Determines how the interface shall be used for that job. Synchronous processing returns with the result while asynchronous processing returns without processing the job. The caller will be notified by the corresponding callback. |    |              |
| <b>Multiplicity</b>              | 1  |    |              |
| <b>Type</b>                      | EcucEnumerationParamDef  |    |              |
| <b>Range</b>                     | CRYPTO_PROCESSING_ASYNC  | -- |              |
|                                  | CRYPTO_PROCESSING_SYNC   | -- |              |
| <b>Post-Build Variant Value</b>  | false  |    |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                                  | <b>Link time</b>   | -- |              |
|                                  | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>        | scope: local   |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00263 :</b>                        |    |              |
| <b>Name</b>                             | CsmInOutRedirectionRef                         |    |              |
| <b>Parent Container</b>                 | CsmJob   |    |              |
| <b>Description</b>                      | This parameter refers to the used redirection. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | Reference to [ CsmInOutRedirections ]          |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                        | X  | All Variants |
|   | <b>Link time</b>                               | -- |              |
|   | <b>Post-build time</b>                         | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                        | X  | All Variants |
|   | <b>Link time</b>                               | -- |              |
|   | <b>Post-build time</b>                         | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                   |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00126 :</b>   |    |              |
| <b>Name</b>                             | CsmJobKeyRef  |    |              |
| <b>Parent Container</b>                 | CsmJob  |    |              |
| <b>Description</b>                      | This parameter refers to the key which shall be used for the CsmPrimitive. It's possible to use a CsmKey for different jobs |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | Reference to [ CsmKey ]   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00123 :</b>  |    |              |
| <b>Name</b>                             | CsmJobPrimitiveCallbackRef   |    |              |
| <b>Parent Container</b>                 | CsmJob   |    |              |
| <b>Description</b>                      | This parameter refers to the used CsmCallback. The referred CsmCallback is called when the crypto job has been finished. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | Reference to [ CsmCallback ]   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00122 :</b>  |    |              |
| <b>Name</b>                             | CsmJobPrimitiveRef   |    |              |
| <b>Parent Container</b>                 | CsmJob   |    |              |
| <b>Description</b>                      | This parameter refers to the used CsmPrimitive. Different jobs may refer to one CsmPrimitive. The referred CsmPrimitive provides detailed information on the actual cryptographic routine. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | Reference to [ CsmPrimitives ]   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|                         |   |  |  |
|-------------------------|---|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00125 :</b>   |  |  |
| <b>Name</b>             | CsmJobQueueRef  |  |  |
| <b>Parent Container</b> | CsmJob  |  |  |
| <b>Description</b>      | This parameter refers to the queue. The queue is used if the underlying crypto driver object is busy. The queue refers also to the channel which is used. |  |  |
| <b>Multiplicity</b>     | 1   |  |  |

|   |                           |    |              |
|---|---------------------------|----|--------------|
| <b>Type</b>                             | Reference to [ CsmQueue ] |    |              |
| <b>Post-Build Variant Value</b>         | false                     |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>          | -- |              |
|   | <b>Post-build time</b>    | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>          | -- |              |
|   | <b>Post-build time</b>    | -- |              |
| <b>Scope / Dependency</b>               | scope: local              |    |              |

**No Included Containers**

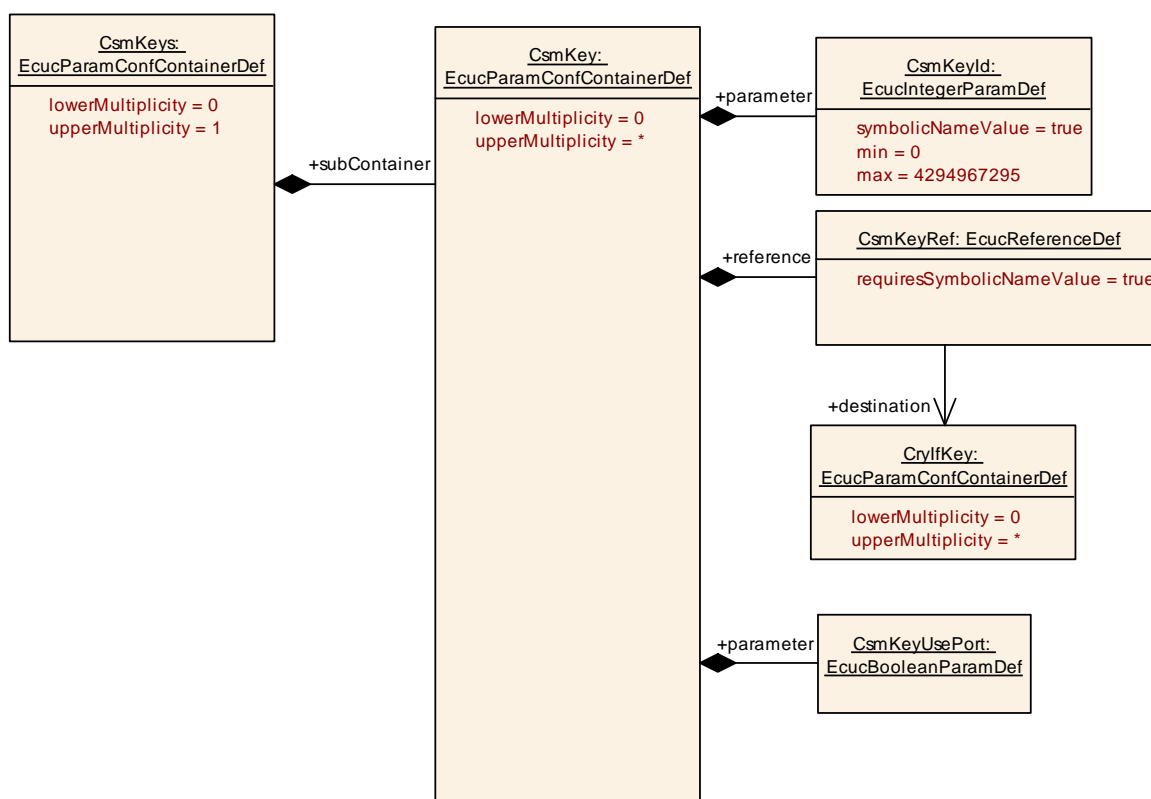


Figure 9-6 Crypto Service Manager Keys Layout

### 10.2.5 CsmKeys

|                                 |                                       |
|---------------------------------|---------------------------------------|
| <b>SWS Item</b>                 | ECUC_Csm_00005 :                      |
| <b>Container Name</b>           | CsmKeys                               |
| <b>Parent Container</b>         | Csm                                   |
| <b>Description</b>              | Container for CSM key configurations. |
| <b>Configuration Parameters</b> |                                       |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmKey                     | 0..*                | Container for configuration of a CSM key. The container name serves as a symbolic name for the identifier of a key configuration. |

### 10.2.6 CsmKey

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00014 :</b>   |
| <b>Container Name</b>           | CsmKey  |
| <b>Parent Container</b>         | CsmKeys   |
| <b>Description</b>              | Container for configuration of a CSM key. The container name serves as a symbolic name for the identifier of a key configuration. |
| <b>Configuration Parameters</b> |   |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00015 :</b>  |    |              |
| <b>Name</b>                             | CsmKeyId   |    |              |
| <b>Parent Container</b>                 | CsmKey   |    |              |
| <b>Description</b>                      | Identifier of the CsmKey. The set of actually configured identifiers shall be consecutive and gapless. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef (Symbolic Name generated for this parameter)                                       |    |              |
| <b>Range</b>                            | 0 .. 4294967295  |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00127 :</b>   |    |              |
| <b>Name</b>                             | CsmKeyUsePort   |    |              |
| <b>Parent Container</b>                 | CsmKey  |    |              |
| <b>Description</b>                      | Does the key need RTE interfaces?<br>True: RTE interfaces used for this key<br>False: No RTE interfaces used for this key |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucBooleanParamDef   |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                         |  |  |  |
|-------------------------|--|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00016 :</b>  |  |  |
| <b>Name</b>             | CsmKeyRef  |  |  |
| <b>Parent Container</b> | CsmKey   |  |  |
| <b>Description</b>      | This parameter refers to the used CryIfKey. The underlying CryIfKey refers to a specific CryptoKey in the Crypto Driver. |  |  |
| <b>Multiplicity</b>     | 1  |  |  |
| <b>Type</b>             | Symbolic name reference to [ CryIfKey ]  |  |  |

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

**No Included Containers**

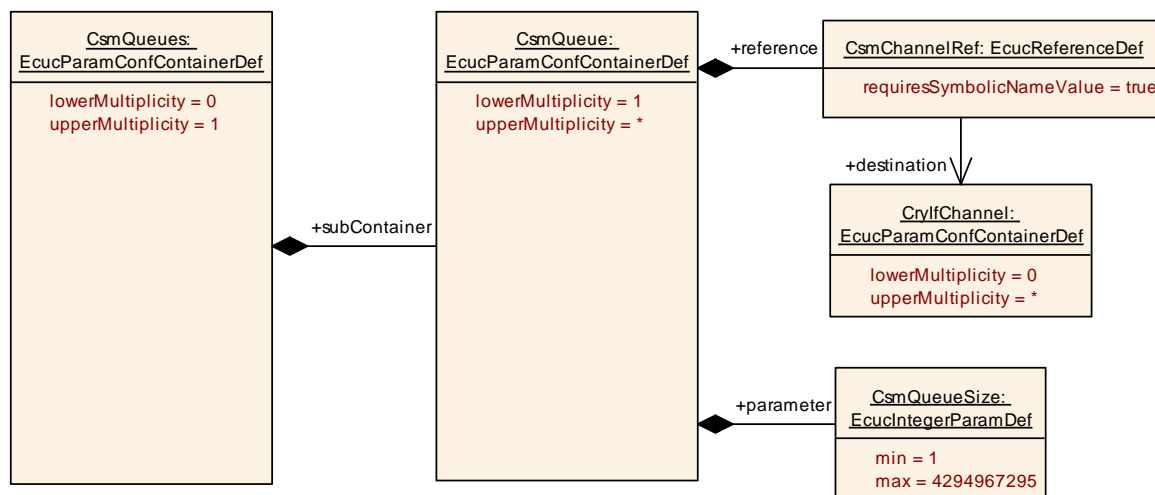


Figure 9-7 Crypto Service Manager Queues Layout

### 10.2.7 CsmQueues

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | ECUC_Csm_00007 :                       |
| <b>Container Name</b>           | CsmQueues                              |
| <b>Parent Container</b>         | Csm                                    |
| <b>Description</b>              | Container for CSM queue configurations |
| <b>Configuration Parameters</b> |  |

| Included Containers |              |   |
|---------------------|--------------|---|
| Container Name      | Multiplicity | Scope / Dependency  |
| CsmQueue            | 1..*         | Container for configuration of a CSM queue.<br>A queue has two tasks:<br>1. queue jobs which cannot be processed since the underlying hardware is busy and<br>2. refer to channel which shall be used |

### 10.2.8 CsmQueue

|                         |                  |
|-------------------------|------------------|
| <b>SWS Item</b>         | ECUC_Csm_00032 : |
| <b>Container Name</b>   | CsmQueue         |
| <b>Parent Container</b> | CsmQueues        |

|                                 |   |
|---------------------------------|---|
| <b>Description</b>              | Container for configuration of a CSM queue.<br>A queue has two tasks:<br>1. queue jobs which cannot be processed since the underlying hardware is busy and<br>2. refer to channel which shall be used |
| <b>Configuration Parameters</b> |   |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00034 :</b>   |    |              |
| <b>Name</b>                             | CsmQueueSize  |    |              |
| <b>Parent Container</b>                 | CsmQueue  |    |              |
| <b>Description</b>                      | Size of the CsmQueue. If jobs cannot be processed by the underlying hardware since the hardware is busy, the jobs stay in the prioritized queue. If the queue is full, the next job will be rejected. |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef   |    |              |
| <b>Range</b>                            | 1 .. 4294967295   |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00033 :</b>                            |    |              |
| <b>Name</b>                             | CsmChannelRef                                      |    |              |
| <b>Parent Container</b>                 | CsmQueue   |    |              |
| <b>Description</b>                      | Refers to the underlying Crypto Interface channel. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | Symbolic name reference to [ CryIfChannel ]        |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                            | X  | All Variants |
|   | <b>Link time</b>                                   | -- |              |
|   | <b>Post-build time</b>                             | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                            | X  | All Variants |
|   | <b>Link time</b>                                   | -- |              |
|   | <b>Post-build time</b>                             | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                       |    |              |

|                               |
|-------------------------------|
| <b>No Included Containers</b> |
|-------------------------------|

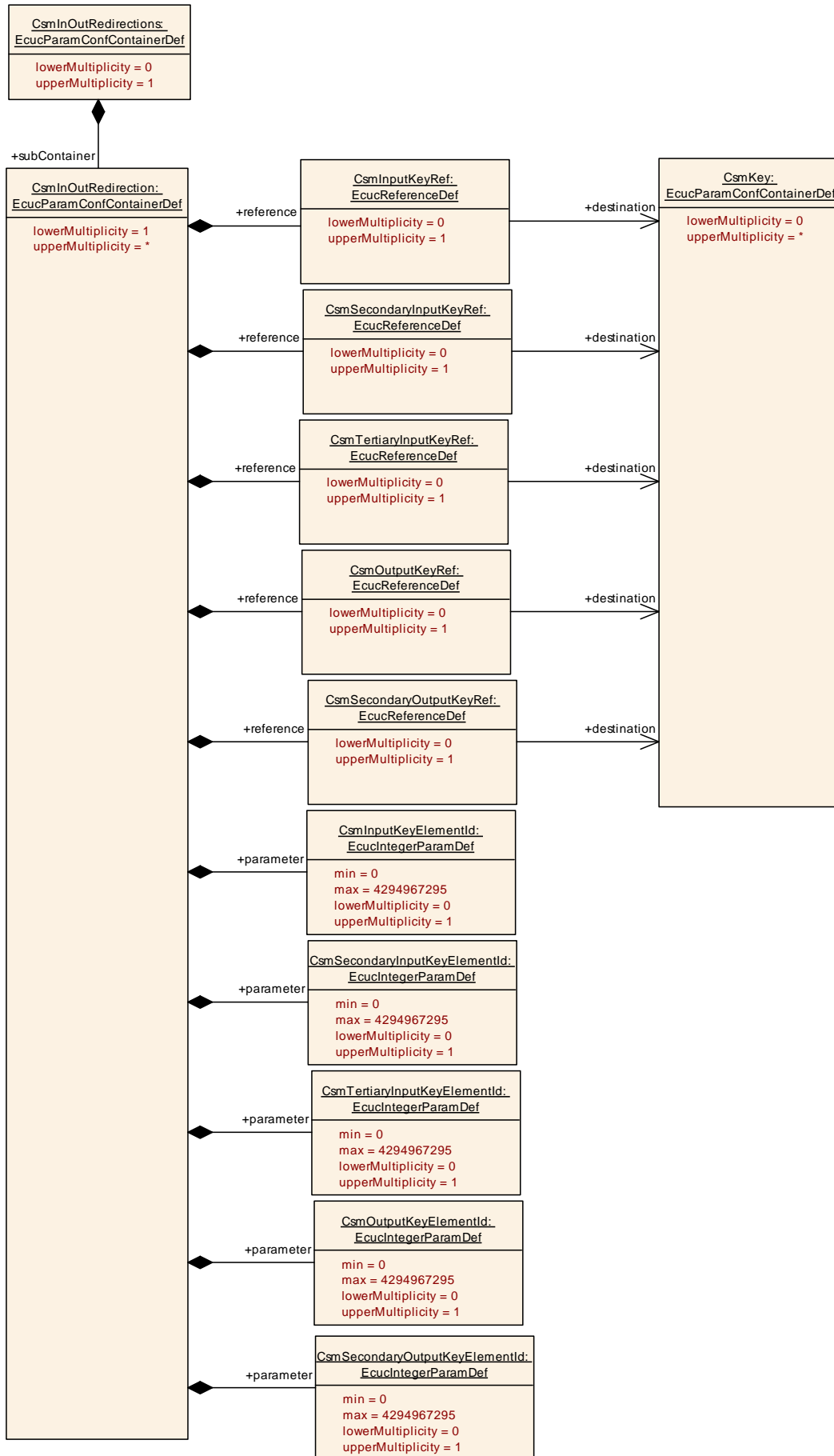




Figure 9-8 Crypto Service Manager CsmInOutRedirections Layout

### 10.2.9 CsmInOutRedirections

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00262 :</b>                          |
| <b>Container Name</b>           | CsmInOutRedirections                             |
| <b>Parent Container</b>         | Csm  |
| <b>Description</b>              | Configuration for CSM redirection configurations |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmInOutRedirection        | 1..*                | Container for configuration of a CSM redirection.<br>A redirection let a CSM job use a specific key element as input or/and output. |

### 10.2.10 CsmInOutRedirection

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00264 :</b>   |
| <b>Container Name</b>           | CsmInOutRedirection   |
| <b>Parent Container</b>         | CsmInOutRedirections  |
| <b>Description</b>              | Container for configuration of a CSM redirection.<br>A redirection let a CSM job use a specific key element as input or/and output. |
| <b>Configuration Parameters</b> |   |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00266 :</b>                     |    |              |
| <b>Name</b>                             | CsmInputKeyElementId                        |    |              |
| <b>Parent Container</b>                 | CsmInOutRedirection                         |    |              |
| <b>Description</b>                      | Identifier of the key element used as input |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcuIntegerParamDef                          |    |              |
| <b>Range</b>                            | 0 .. 4294967295                             |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant</b>               | false                                       |    |              |
| <b>Multiplicity</b>                     | false                                       |    |              |
| <b>Post-Build Variant Value</b>         | false                                       |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|   | <b>Link time</b>                            | -- |              |
|   | <b>Post-build time</b>                      | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                     | X  | All Variants |
|   | <b>Link time</b>                            | -- |              |
|   | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                |    |              |

|                         |   |  |  |
|-------------------------|---|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00272 :</b>                       |  |  |
| <b>Name</b>             | CsmOutputKeyElementId                         |  |  |
| <b>Parent Container</b> | CsmInOutRedirection                           |  |  |
| <b>Description</b>      | Identifier of the key element used as output. |  |  |
| <b>Multiplicity</b>     | 0..1  |  |  |
| <b>Type</b>             | EcuIntegerParamDef                            |  |  |
| <b>Range</b>            | 0 .. 4294967295                               |  |  |

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

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00269 :</b>                                |    |              |
| <b>Name</b>                             | CsmSecondaryInputKeyElementId                          |    |              |
| <b>Parent Container</b>                 | CsmInOutRedirection                                    |    |              |
| <b>Description</b>                      | Identifier of the key element used as secondary input. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                                    |    |              |
| <b>Range</b>                            | 0 .. 4294967295  |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                | X  | All Variants |
|   | <b>Link time</b>                                       | -- |              |
|   | <b>Post-build time</b>                                 | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                | X  | All Variants |
|   | <b>Link time</b>                                       | -- |              |
|   | <b>Post-build time</b>                                 | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00274 :</b>                                 |    |              |
| <b>Name</b>                             | CsmSecondaryOutputKeyElementId                          |    |              |
| <b>Parent Container</b>                 | CsmInOutRedirection                                     |    |              |
| <b>Description</b>                      | Identifier of the key element used as secondary output. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                                     |    |              |
| <b>Range</b>                            | 0 .. 4294967295   |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                 | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                 | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                         |   |  |  |
|-------------------------|---|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00270 :</b>                               |  |  |
| <b>Name</b>             | CsmTertiaryInputKeyElementId                          |  |  |
| <b>Parent Container</b> | CsmInOutRedirection                                   |  |  |
| <b>Description</b>      | Identifier of the key element used as tertiary input. |  |  |
| <b>Multiplicity</b>     | 0..1  |  |  |
| <b>Type</b>             | EcucIntegerParamDef                                   |  |  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Range</b>                            | 0 .. 4294967295         |    |              |
| <b>Default value</b>                    | --                      |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false                   |    |              |
| <b>Post-Build Variant Value</b>         | false                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00265 :</b>                         |    |              |
| <b>Name</b>                             | CsmInputKeyRef                                  |    |              |
| <b>Parent Container</b>                 | CsmInOutRedirection                             |    |              |
| <b>Description</b>                      | This parameter refers to the key used as input. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | Reference to [ CsmKey ]                         |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                         | X  | All Variants |
|   | <b>Link time</b>                                | -- |              |
|   | <b>Post-build time</b>                          | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                         | X  | All Variants |
|   | <b>Link time</b>                                | -- |              |
|   | <b>Post-build time</b>                          | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                    |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00271 :</b>                          |    |              |
| <b>Name</b>                             | CsmOutputKeyRef                                  |    |              |
| <b>Parent Container</b>                 | CsmInOutRedirection                              |    |              |
| <b>Description</b>                      | This parameter refers to the key used as output. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | Reference to [ CsmKey ]                          |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                          | X  | All Variants |
|   | <b>Link time</b>                                 | -- |              |
|   | <b>Post-build time</b>                           | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                          | X  | All Variants |
|   | <b>Link time</b>                                 | -- |              |
|   | <b>Post-build time</b>                           | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                     |    |              |

|  |   |  |  |
|--|---|--|--|
| <b>SWS Item</b>                        | <b>ECUC_Csm_00267 :</b>                                   |  |  |
| <b>Name</b>                            | CsmSecondaryInputKeyRef                                   |  |  |
| <b>Parent Container</b>                | CsmInOutRedirection                                       |  |  |
| <b>Description</b>                     | This parameter refers to the key used as secondary input. |  |  |
| <b>Multiplicity</b>                    | 0..1  |  |  |
| <b>Type</b>                            | Reference to [ CsmKey ]                                   |  |  |
| <b>Post-Build Variant Multiplicity</b> | false   |  |  |
| <b>Post-Build Variant Value</b>        | false   |  |  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00273 :</b>                                    |    |              |
| <b>Name</b>                             | CsmSecondaryOutputKeyRef                                   |    |              |
| <b>Parent Container</b>                 | CsmInOutRedirection  |    |              |
| <b>Description</b>                      | This parameter refers to the key used as secondary output. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | Reference to [ CsmKey ]                                    |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                    | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>                                     | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                    | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>                                     | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00268 :</b>                                  |    |              |
| <b>Name</b>                             | CsmTertiaryInputKeyRef                                   |    |              |
| <b>Parent Container</b>                 | CsmInOutRedirection                                      |    |              |
| <b>Description</b>                      | This parameter refers to the key used as tertiary input. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | Reference to [ CsmKey ]                                  |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>                                   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>                                   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

**No Included Containers**

### 10.2.11 CsmPrimitives

|                                 |  |  |  |
|---------------------------------|--|--|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00006 :</b>                      |  |  |
| <b>Container Name</b>           | CsmPrimitives                                |  |  |
| <b>Parent Container</b>         | Csm  |  |  |
| <b>Description</b>              | Container for configuration of CsmPrimitives |  |  |
| <b>Configuration Parameters</b> |  |  |  |

**Included Containers**

| <b>Container Name</b>       | <b>Multiplicity</b> | <b>Scope / Dependency</b>                          |
|-----------------------------|---------------------|--|
| CsmAEADDecrypt              | 0..1                | Configuration of AEAD decryption primitives        |
| CsmAEADEncrypt              | 0..1                | Configuration of AEAD encryption primitives        |
| CsmDecrypt                  | 0..1                | Configurations of Decryption primitives            |
| CsmEncrypt                  | 0..1                | Configurations of Encryption primitives            |
| CsmHash                     | 0..1                | Container for Hash Configurations                  |
| CsmJobKeyDerive             | 0..1                | Configurations of KeyDerive primitives             |
| CsmJobKeyExchangeCalcPubVal | 0..1                | Configurations of KeyExchangeCalcPubVal primitives |
| CsmJobKeyExchangeCalcSecret | 0..1                | Configurations of KeyExchangeCalcSecret primitives |
| CsmJobKeyGenerate           | 0..1                | Configurations of KeyGenerate primitives           |
| CsmJobKeySetValid           | 0..1                | Configurations of KeySetValid primitives           |
| CsmJobRandomSeed            | 0..1                | Configurations of RandomSeed primitives            |
| CsmMacGenerate              | 0..1                | Configurations of MacGenerate primitives           |
| CsmMacVerify                | 0..1                | Configurations of MacVerify primitives             |
| CsmRandomGenerate           | 0..1                | Configurations of RandomGenerate primitives        |
| CsmSignatureGenerate        | 0..1                | Configurations of SignatureGenerate primitives     |
| CsmSignatureVerify          | 0..1                | Configurations of SignatureVerify primitives       |

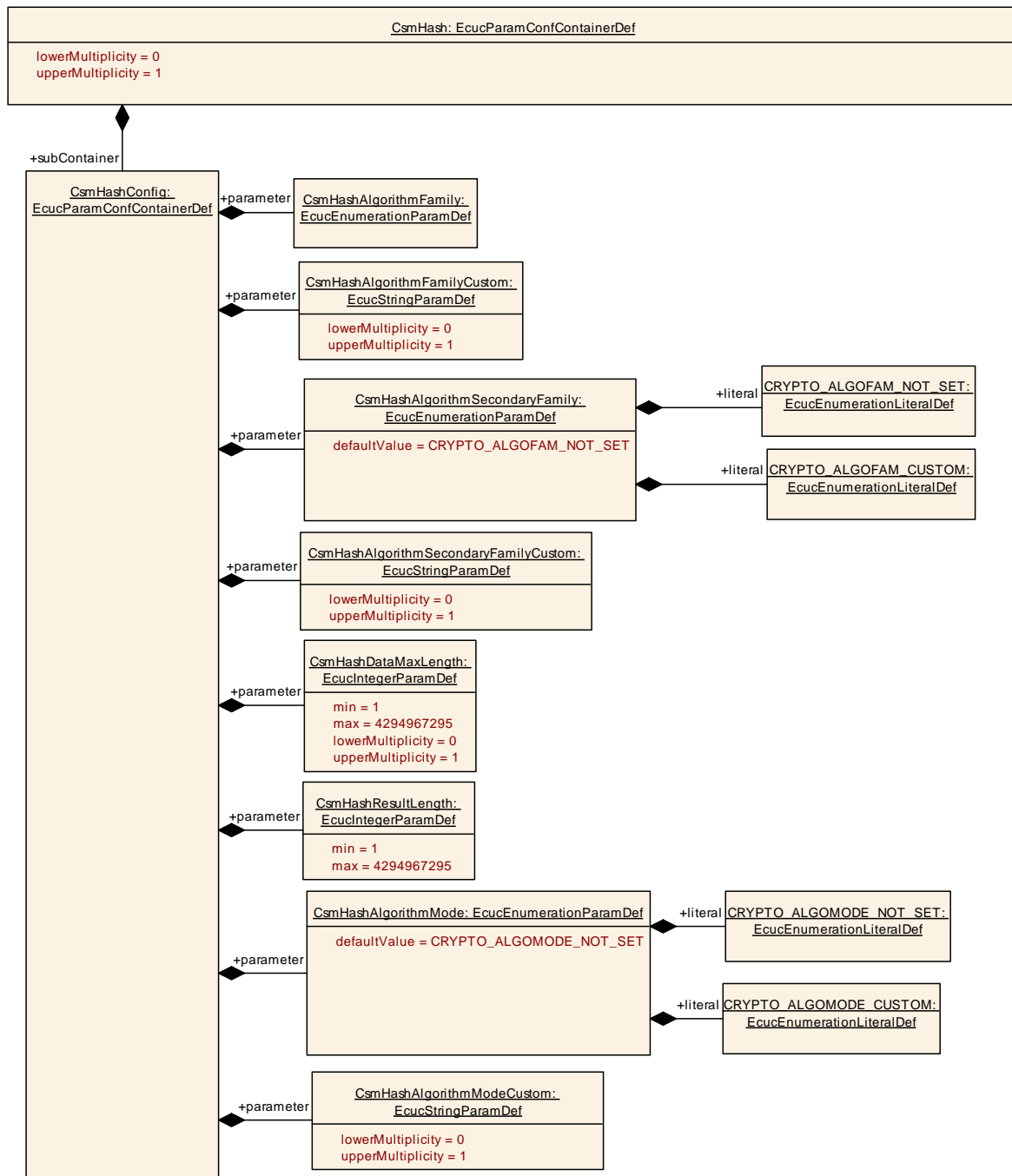


Figure 9-9 CsmHash Layout

10.2.12 CsmHash

|                                 |                                   |
|---------------------------------|-----------------------------------|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00021 :</b>           |
| <b>Container Name</b>           | CsmHash                           |
| <b>Parent Container</b>         | CsmPrimitives                     |
| <b>Description</b>              | Container for Hash Configurations |
| <b>Configuration Parameters</b> |                                   |

|                            |                     |                           |
|----------------------------|---------------------|---------------------------|
| <b>Included Containers</b> |                     |                           |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b> |

|               |   |  |
|---------------|---|--|
| CsmHashConfig | 1 | Container for configuration of a CSM hash. The container name serves as a symbolic name for the identifier of a key configuration. |
|---------------|---|--|

### 10.2.13 CsmHashConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00036 :</b>  |
| <b>Container Name</b>           | CsmHashConfig  |
| <b>Parent Container</b>         | CsmHash  |
| <b>Description</b>              | Container for configuration of a CSM hash. The container name serves as a symbolic name for the identifier of a key configuration. |
| <b>Configuration Parameters</b> |  |

|   |   |                |
|---|---|----------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00038 :</b>   |                |
| <b>Name</b>                             | CsmHashAlgorithmFamily  |                |
| <b>Parent Container</b>                 | CsmHashConfig   |                |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |                |
| <b>Multiplicity</b>                     | 1   |                |
| <b>Type</b>                             | EcucEnumerationParamDef   |                |
| <b>Range</b>                            | CRYPTO_ALGOFAM_BLAKE_1_256  | 0x0F           |
|   | CRYPTO_ALGOFAM_BLAKE_1_512  | 0x10           |
|   | CRYPTO_ALGOFAM_BLAKE_2s_256   | 0x11           |
|   | CRYPTO_ALGOFAM_BLAKE_2s_512   | 0x12           |
|   | CRYPTO_ALGOFAM_CUSTOM   | 0xFF           |
|   | CRYPTO_ALGOFAM_RIPEMD160  | 0x0E           |
|   | CRYPTO_ALGOFAM_SHA1   | 0x01           |
|   | CRYPTO_ALGOFAM_SHA2_224   | 0x02           |
|   | CRYPTO_ALGOFAM_SHA2_256   | 0x03           |
|   | CRYPTO_ALGOFAM_SHA2_384   | 0x04           |
|   | CRYPTO_ALGOFAM_SHA2_512   | 0x05           |
|   | CRYPTO_ALGOFAM_SHA2_512_224   | 0x06           |
|   | CRYPTO_ALGOFAM_SHA2_512_256   | 0x07           |
|   | CRYPTO_ALGOFAM_SHA3_224   | 0x08           |
|   | CRYPTO_ALGOFAM_SHA3_256   | 0x09           |
|   | CRYPTO_ALGOFAM_SHA3_384   | 0x0A           |
|   | CRYPTO_ALGOFAM_SHA3_512   | 0x0B           |
|   | CRYPTO_ALGOFAM_SHAKE128   | 0x0C           |
|   | CRYPTO_ALGOFAM_SHAKE256   | 0x0D           |
| <b>Post-Build Variant Value</b>         | false   |                |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X All Variants |
|   | <b>Link time</b>  | --             |
|   | <b>Post-build time</b>  | --             |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X All Variants |
|   | <b>Link time</b>  | --             |
|   | <b>Post-build time</b>  | --             |
| <b>Scope / Dependency</b>               | scope: local  |                |

|                 |                              |
|-----------------|------------------------------|
| <b>SWS Item</b> | <b>ECUC_Csm_00128 :</b>      |
| <b>Name</b>     | CsmHashAlgorithmFamilyCustom |

|   |  |    |              |
|---|--|----|--------------|
| <b>Parent Container</b>                 | CsmHashConfig  |    |              |
| <b>Description</b>                      | This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmHashAlgorithmFamily. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucStringParamDef   |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00131 :</b>                                   |    |              |
| <b>Name</b>                             | CsmHashAlgorithmMode                                      |    |              |
| <b>Parent Container</b>                 | CsmHashConfig   |    |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |    |              |
| <b>Range</b>                            | CRYPTO_ALGOMODE_CUSTOM                                    |    | 0xFF         |
|   | CRYPTO_ALGOMODE_NOT_SET                                   |    | 0x00         |
| <b>Default value</b>                    | CRYPTO_ALGOMODE_NOT_SET                                   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |                                    |    |              |
|---|------------------------------------|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00132 :</b>            |    |              |
| <b>Name</b>                             | CsmHashAlgorithmModeCustom         |    |              |
| <b>Parent Container</b>                 | CsmHashConfig                      |    |              |
| <b>Description</b>                      | Name of the custom primitive mode. |    |              |
| <b>Multiplicity</b>                     | 0..1                               |    |              |
| <b>Type</b>                             | EcucStringParamDef                 |    |              |
| <b>Default value</b>                    | --                                 |    |              |
| <b>maxLength</b>                        | --                                 |    |              |
| <b>minLength</b>                        | --                                 |    |              |
| <b>regularExpression</b>                | --                                 |    |              |
| <b>Post-Build Variant Value</b>         | false                              |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>            | X  | All Variants |
|   | <b>Link time</b>                   | -- |              |
|   | <b>Post-build time</b>             | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>            | X  | All Variants |
|   | <b>Link time</b>                   | -- |              |
|   | <b>Post-build time</b>             | -- |              |
| <b>Scope / Dependency</b>               | scope: local                       |    |              |



|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00181 :</b>                                     |    |              |
| <b>Name</b>                             | CsmHashAlgorithmSecondaryFamily                             |    |              |
| <b>Parent Container</b>                 | CsmHashConfig   |    |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                     |    |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_CUSTOM                                       |    | 0xFF         |
|   | CRYPTO_ALGOFAM_NOT_SET                                      |    | 0x00         |
| <b>Default value</b>                    | CRYPTO_ALGOFAM_NOT_SET                                      |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                     | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                      | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                     | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                      | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00129 :</b>   |    |              |
| <b>Name</b>                             | CsmHashAlgorithmSecondaryFamilyCustom   |    |              |
| <b>Parent Container</b>                 | CsmHashConfig   |    |              |
| <b>Description</b>                      | This is the second name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is set as CsmHashAlgorithmSecondaryFamily. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00040 :</b>                    |    |              |
| <b>Name</b>                             | CsmHashDataMaxLength                       |    |              |
| <b>Parent Container</b>                 | CsmHashConfig                              |    |              |
| <b>Description</b>                      | Max size of the input data length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1                                       |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                        |    |              |
| <b>Range</b>                            | 1 .. 4294967295                            |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Value</b>         | false                                      |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                    | X  | All Variants |
|   | <b>Link time</b>                           | -- |              |
|   | <b>Post-build time</b>                     | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                    | X  | All Variants |
|   | <b>Link time</b>                           | -- |              |

|                           |                        |    |  |
|---------------------------|------------------------|----|--|
|                           | <b>Post-build time</b> | -- |  |
| <b>Scope / Dependency</b> | scope: local           |    |  |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00130 :</b>                 |    |              |
| <b>Name</b>                             | CsmHashResultLength                     |    |              |
| <b>Parent Container</b>                 | CsmHashConfig                           |    |              |
| <b>Description</b>                      | Size of the output hash length in bytes |    |              |
| <b>Multiplicity</b>                     | 1                                       |    |              |
| <b>Type</b>                             | EcuIntegerParamDef                      |    |              |
| <b>Range</b>                            | 1 .. 4294967295                         |    |              |
| <b>Default value</b>                    | --                                      |    |              |
| <b>Post-Build Variant Value</b>         | false                                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                 | X  | All Variants |
|   | <b>Link time</b>                        | -- |              |
|   | <b>Post-build time</b>                  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                 | X  | All Variants |
|   | <b>Link time</b>                        | -- |              |
|   | <b>Post-build time</b>                  | -- |              |
| <b>Scope / Dependency</b>               | scope: local                            |    |              |

**No Included Containers**

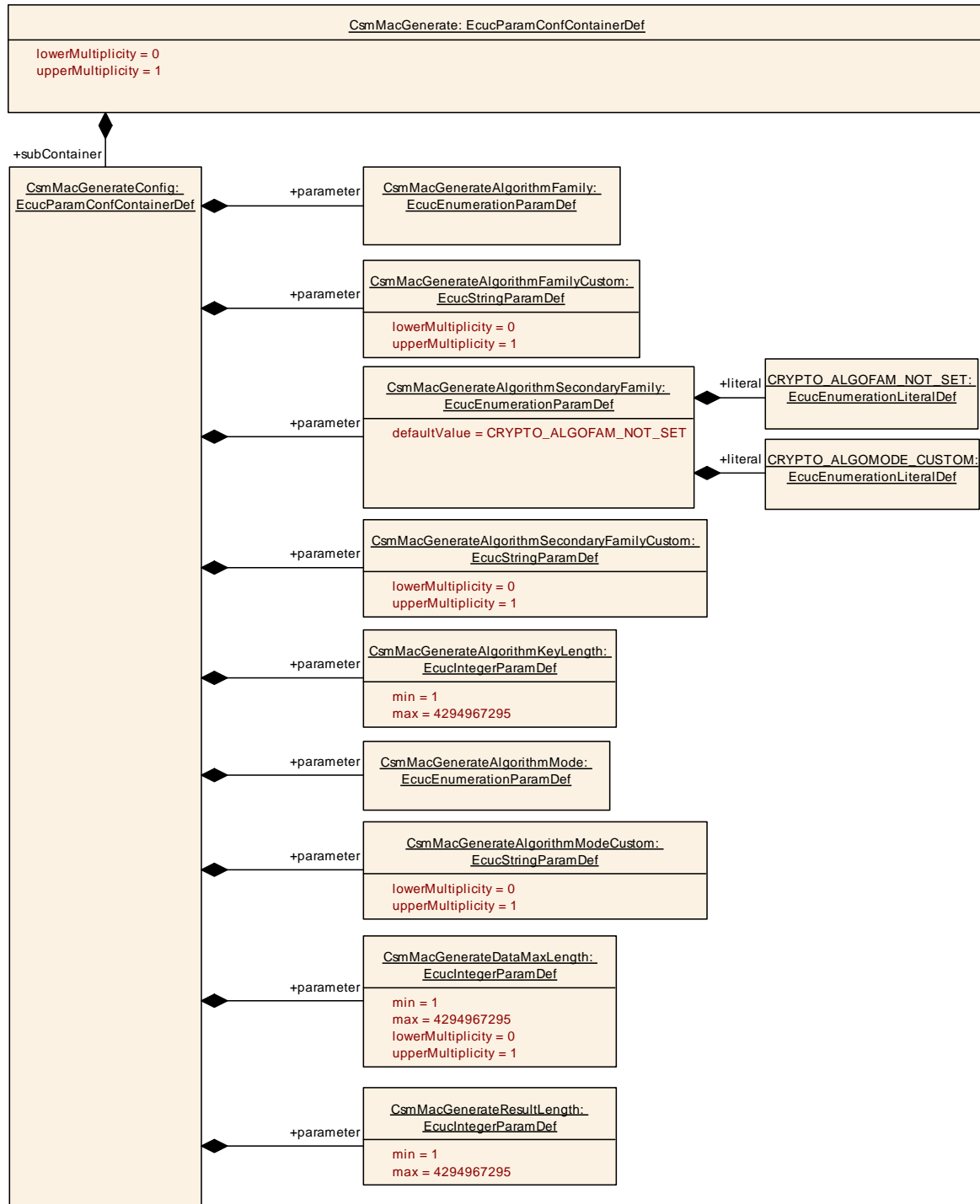


Figure 9-10 CsmMacGenerate Layout

10.2.14 CsmMacGenerate

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00022 :</b>                  |
| <b>Container Name</b>           | CsmMacGenerate                           |
| <b>Parent Container</b>         | CsmPrimitives                            |
| <b>Description</b>              | Configurations of MacGenerate primitives |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmMacGenerateConfig       | 1                   | 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. |

### 10.2.15 CsmMacGenerateConfig

| <b>SWS Item</b>                 |   | <b>ECUC_Csm_00041 :</b> |
|---------------------------------|---|-------------------------|
| <b>Container Name</b>           | CsmMacGenerateConfig  |                         |
| <b>Parent Container</b>         | CsmMacGenerate  |                         |
| <b>Description</b>              | 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. |                         |
| <b>Configuration Parameters</b> |   |                         |

| <b>SWS Item</b>                         |   | <b>ECUC_Csm_00188 :</b> |              |
|---|---|-------------------------|--------------|
| <b>Name</b>                             | CsmMacGenerateAlgorithmFamily   |                         |              |
| <b>Parent Container</b>                 | CsmMacGenerateConfig  |                         |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |                         |              |
| <b>Multiplicity</b>                     | 1   |                         |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |                         |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_3DES   |                         | 0x13         |
|   | CRYPTO_ALGOFAM_AES  |                         | 0x14         |
|   | CRYPTO_ALGOFAM_BLAKE_1_256  |                         | 0x0F         |
|   | CRYPTO_ALGOFAM_BLAKE_1_512  |                         | 0x10         |
|   | CRYPTO_ALGOFAM_BLAKE_2s_256   |                         | 0x11         |
|   | CRYPTO_ALGOFAM_BLAKE_2s_512   |                         | 0x12         |
|   | CRYPTO_ALGOFAM_CHACHA   |                         | 0x15         |
|   | CRYPTO_ALGOFAM_CUSTOM   |                         | 0xFF         |
|   | CRYPTO_ALGOFAM_RIPEMD160  |                         | 0x0E         |
|   | CRYPTO_ALGOFAM_RNG  |                         | 0x1B         |
|   | CRYPTO_ALGOFAM_SHA1   |                         | 0x01         |
|   | CRYPTO_ALGOFAM_SHA2_224   |                         | 0x02         |
|   | CRYPTO_ALGOFAM_SHA2_256   |                         | 0x03         |
|   | CRYPTO_ALGOFAM_SHA2_384   |                         | 0x04         |
|   | CRYPTO_ALGOFAM_SHA2_512   |                         | 0x05         |
|   | CRYPTO_ALGOFAM_SHA2_512_224   |                         | 0x06         |
|   | CRYPTO_ALGOFAM_SHA2_512_256   |                         | 0x07         |
|   | CRYPTO_ALGOFAM_SHA3_224   |                         | 0x08         |
|   | CRYPTO_ALGOFAM_SHA3_256   |                         | 0x09         |
|   | CRYPTO_ALGOFAM_SHA3_384   |                         | 0x0A         |
|   | CRYPTO_ALGOFAM_SHA3_512   |                         | 0x0B         |
|   | CRYPTO_ALGOFAM_SHAKE128   |                         | 0x0C         |
|   | CRYPTO_ALGOFAM_SHAKE256   |                         | 0x0D         |
| CRYPTO_ALGOFAM_SIPHASH                  |   | 0x1C                    |              |
| <b>Post-Build Variant Value</b>         | false   |                         |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X                       | All Variants |
|   | <b>Link time</b>  | --                      |              |
|   | <b>Post-build time</b>  | --                      |              |
| <b>Value</b>                            | <b>Pre-compile time</b>   | X                       | All Variants |

|                            |                        |    |  |
|----------------------------|------------------------|----|--|
| <b>Configuration Class</b> | <b>Link time</b>       | -- |  |
|                            | <b>Post-build time</b> | -- |  |
| <b>Scope / Dependency</b>  | scope: local           |    |  |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00133 :</b>  |    |              |
| <b>Name</b>                             | CsmMacGenerateAlgorithmFamilyCustom  |    |              |
| <b>Parent Container</b>                 | CsmMacGenerateConfig   |    |              |
| <b>Description</b>                      | This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmMacGenerateAlgorithmFamily |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucStringParamDef   |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |                                  |    |              |
|---|----------------------------------|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00044 :</b>          |    |              |
| <b>Name</b>                             | CsmMacGenerateAlgorithmKeyLength |    |              |
| <b>Parent Container</b>                 | CsmMacGenerateConfig             |    |              |
| <b>Description</b>                      | Size of the MAC key in bytes     |    |              |
| <b>Multiplicity</b>                     | 1                                |    |              |
| <b>Type</b>                             | EcucIntegerParamDef              |    |              |
| <b>Range</b>                            | 1 .. 4294967295                  |    |              |
| <b>Default value</b>                    | --                               |    |              |
| <b>Post-Build Variant Value</b>         | false                            |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>          | X  | All Variants |
|   | <b>Link time</b>                 | -- |              |
|   | <b>Post-build time</b>           | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>          | X  | All Variants |
|   | <b>Link time</b>                 | -- |              |
|   | <b>Post-build time</b>           | -- |              |
| <b>Scope / Dependency</b>               | scope: local                     |    |              |

|                         |   |  |      |
|-------------------------|---|--|------|
| <b>SWS Item</b>         | <b>ECUC_Csm_00189 :</b>                                   |  |      |
| <b>Name</b>             | CsmMacGenerateAlgorithmMode                               |  |      |
| <b>Parent Container</b> | CsmMacGenerateConfig                                      |  |      |
| <b>Description</b>      | Determines the algorithm mode used for the crypto service |  |      |
| <b>Multiplicity</b>     | 1   |  |      |
| <b>Type</b>             | EcucEnumerationParamDef                                   |  |      |
| <b>Range</b>            | CRYPTO_ALGOMODE_CMACE                                     |  | 0x10 |
|                         | CRYPTO_ALGOMODE_CTRDRBG                                   |  | 0x12 |
|                         | CRYPTO_ALGOMODE_CUSTOM                                    |  | 0xFF |
|                         | CRYPTO_ALGOMODE_GMAC                                      |  | 0x11 |
|                         | CRYPTO_ALGOMODE_HMAC                                      |  | 0x0f |
|                         | CRYPTO_ALGOMODE_NOT_SET                                   |  | 0x00 |
|                         | CRYPTO_ALGOMODE_SIPHASH_2_4                               |  | 0x17 |

|   |                             |                |
|---|-----------------------------|----------------|
|   | CRYPTO_ALGOMODE_SIPHASH_4_8 | 0x18           |
| <b>Post-Build Variant Value</b>         | false                       |                |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>     | X All Variants |
|   | <b>Link time</b>            | --             |
|   | <b>Post-build time</b>      | --             |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>     | X All Variants |
|   | <b>Link time</b>            | --             |
|   | <b>Post-build time</b>      | --             |
| <b>Scope / Dependency</b>               | scope: local                |                |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00136 :</b>                                       |    |              |
| <b>Name</b>                             | CsmMacGenerateAlgorithmModeCustom                             |    |              |
| <b>Parent Container</b>                 | CsmMacGenerateConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00134 :</b>   |      |              |
| <b>Name</b>                             | CsmMacGenerateAlgorithmSecondaryFamily                                |      |              |
| <b>Parent Container</b>                 | CsmMacGenerateConfig  |      |              |
| <b>Description</b>                      | Determines the secondary algorithm family used for the crypto service |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_NOT_SET  | 0x00 |              |
|   | CRYPTO_ALGOMODE_CUSTOM  | 0xFF |              |
| <b>Default value</b>                    | CRYPTO_ALGOFAM_NOT_SET  |      |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>               | scope: local  |      |              |

|                         |  |  |  |
|-------------------------|--|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00135 :</b>  |  |  |
| <b>Name</b>             | CsmMacGenerateAlgorithmSecondaryFamilyCustom   |  |  |
| <b>Parent Container</b> | CsmMacGenerateConfig   |  |  |
| <b>Description</b>      | This is the second name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is set as |  |  |

|   |  |    |              |
|---|--|----|--------------|
|   | CsmHashAlgorithmSecondaryFamilyCustom. |    |              |
| <b>Multiplicity</b>                     | 0..1                                   |    |              |
| <b>Type</b>                             | EcucStringParamDef                     |    |              |
| <b>Default value</b>                    | --                                     |    |              |
| <b>maxLength</b>                        | --                                     |    |              |
| <b>minLength</b>                        | --                                     |    |              |
| <b>regularExpression</b>                | --                                     |    |              |
| <b>Post-Build Variant Value</b>         | false                                  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                | X  | All Variants |
|   | <b>Link time</b>                       | -- |              |
|   | <b>Post-build time</b>                 | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                | X  | All Variants |
|   | <b>Link time</b>                       | -- |              |
|   | <b>Post-build time</b>                 | -- |              |
| <b>Scope / Dependency</b>               | scope: local                           |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00137 :</b>                    |    |              |
| <b>Name</b>                             | CsmMacGenerateDataMaxLength                |    |              |
| <b>Parent Container</b>                 | CsmMacGenerateConfig                       |    |              |
| <b>Description</b>                      | Max size of the input data length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1                                       |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                        |    |              |
| <b>Range</b>                            | 1 .. 4294967295                            |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Value</b>         | false                                      |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                    | X  | All Variants |
|   | <b>Link time</b>                           | -- |              |
|   | <b>Post-build time</b>                     | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                    | X  | All Variants |
|   | <b>Link time</b>                           | -- |              |
|   | <b>Post-build time</b>                     | -- |              |
| <b>Scope / Dependency</b>               | scope: local                               |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00138 :</b>                |    |              |
| <b>Name</b>                             | CsmMacGenerateResultLength             |    |              |
| <b>Parent Container</b>                 | CsmMacGenerateConfig                   |    |              |
| <b>Description</b>                      | Size of the output MAC length in bytes |    |              |
| <b>Multiplicity</b>                     | 1                                      |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                    |    |              |
| <b>Range</b>                            | 1 .. 4294967295                        |    |              |
| <b>Default value</b>                    | --                                     |    |              |
| <b>Post-Build Variant Value</b>         | false                                  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                | X  | All Variants |
|   | <b>Link time</b>                       | -- |              |
|   | <b>Post-build time</b>                 | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                | X  | All Variants |
|   | <b>Link time</b>                       | -- |              |
|   | <b>Post-build time</b>                 | -- |              |
| <b>Scope / Dependency</b>               | scope: local                           |    |              |

|                               |
|-------------------------------|
| <b>No Included Containers</b> |
|-------------------------------|

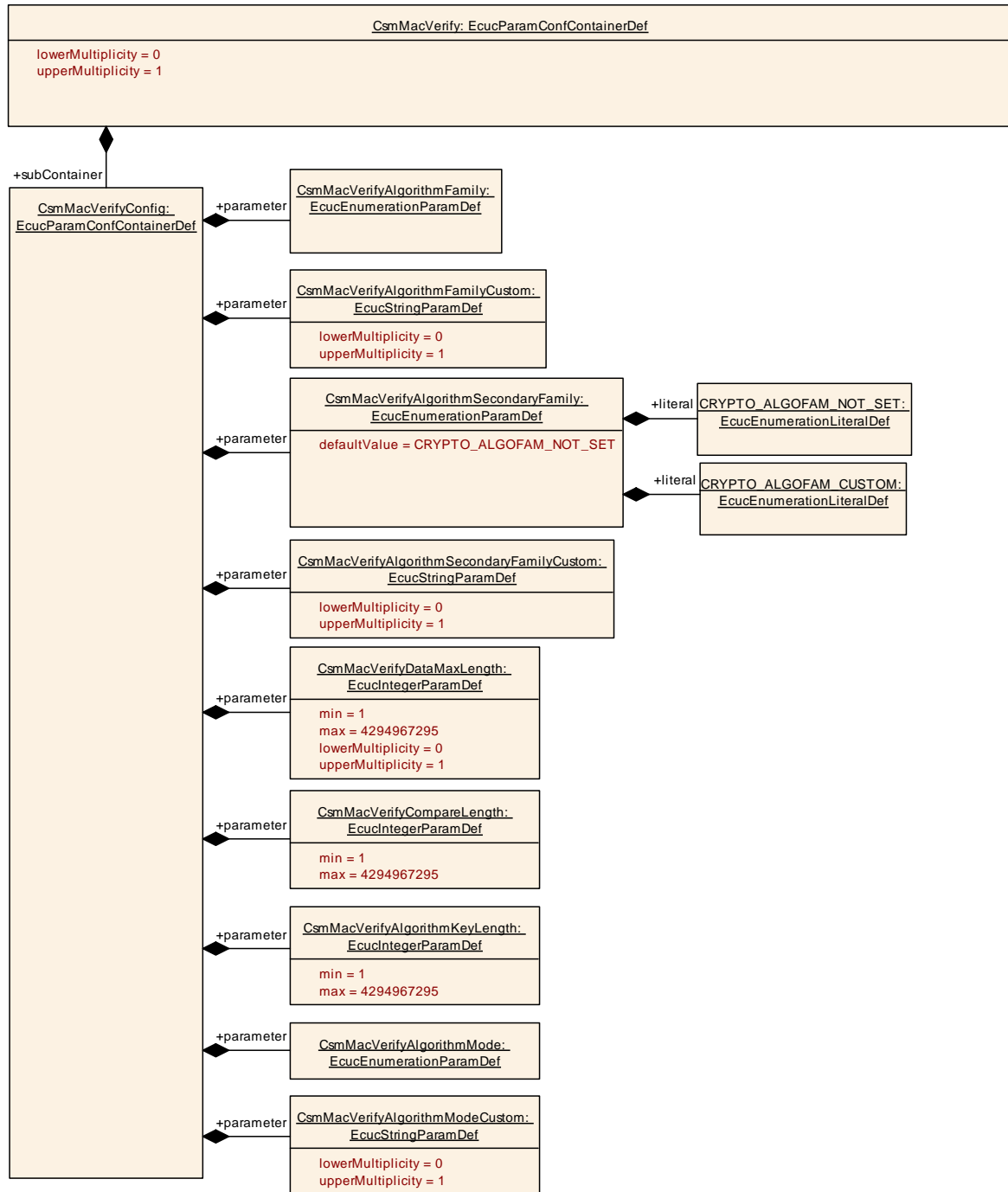


Figure 9-11 CsmMacVerify Layout

10.2.16 CsmMacVerify

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00023 :</b>                |
| <b>Container Name</b>           | CsmMacVerify                           |
| <b>Parent Container</b>         | CsmPrimitives                          |
| <b>Description</b>              | Configurations of MacVerify primitives |
| <b>Configuration Parameters</b> |  |



| <b>Included Containers</b> |                     |  |
|----------------------------|---------------------|--|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>  |
| CsmMacVerifyConfig         | 1                   | 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 |

### 10.2.17 CsmMacVerifyConfig

| <b>SWS Item</b>                 | <b>ECUC_Csm_00049 :</b>  |
|---------------------------------|--|
| <b>Container Name</b>           | CsmMacVerifyConfig   |
| <b>Parent Container</b>         | CsmMacVerify   |
| <b>Description</b>              | 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 |
| <b>Configuration Parameters</b> |  |

| <b>SWS Item</b>                         | <b>ECUC_Csm_00051 :</b>   |                |
|---|---|----------------|
| <b>Name</b>                             | CsmMacVerifyAlgorithmFamily   |                |
| <b>Parent Container</b>                 | CsmMacVerifyConfig  |                |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |                |
| <b>Multiplicity</b>                     | 1   |                |
| <b>Type</b>                             | EcucEnumerationParamDef   |                |
| <b>Range</b>                            | CRYPTO_ALGOFAM_3DES   | 0x13           |
|   | CRYPTO_ALGOFAM_AES  | 0x14           |
|   | CRYPTO_ALGOFAM_BLAKE_1_256  | 0x0F           |
|   | CRYPTO_ALGOFAM_BLAKE_1_512  | 0x10           |
|   | CRYPTO_ALGOFAM_BLAKE_2s_256   | 0x11           |
|   | CRYPTO_ALGOFAM_BLAKE_2s_512   | 0x12           |
|   | CRYPTO_ALGOFAM_CHACHA   | 0x15           |
|   | CRYPTO_ALGOFAM_RIPEMD160  | 0x0E           |
|   | CRYPTO_ALGOFAM_RNG  | 0x1B           |
|   | CRYPTO_ALGOFAM_SHA1   | 0x01           |
|   | CRYPTO_ALGOFAM_SHA2_224   | 0x02           |
|   | CRYPTO_ALGOFAM_SHA2_256   | 0x03           |
|   | CRYPTO_ALGOFAM_SHA2_384   | 0x04           |
|   | CRYPTO_ALGOFAM_SHA2_512   | 0x05           |
|   | CRYPTO_ALGOFAM_SHA2_512_224   | 0x06           |
|   | CRYPTO_ALGOFAM_SHA2_512_256   | 0x07           |
|   | CRYPTO_ALGOFAM_SHA3_224   | 0x08           |
|   | CRYPTO_ALGOFAM_SHA3_256   | 0x09           |
|   | CRYPTO_ALGOFAM_SHA3_384   | 0x0A           |
|   | CRYPTO_ALGOFAM_SHA3_512   | 0x0B           |
|   | CRYPTO_ALGOFAM_SHAKE128   | 0x0C           |
|   | CRYPTO_ALGOFAM_SHAKE256   | 0x0D           |
|   | CRYPTO_ALGOFAM_SIPHASH  | 0x1C           |
| CRYPTO_ALGOMODE_CUSTOM                  | 0xFF  |                |
| <b>Post-Build Variant Value</b>         | false   |                |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X All Variants |
|   | <b>Link time</b>  | --             |
|   | <b>Post-build time</b>  | --             |
| <b>Value</b>                            | <b>Pre-compile time</b>   | X All Variants |

|                            |                        |    |  |
|----------------------------|------------------------|----|--|
| <b>Configuration Class</b> | <b>Link time</b>       | -- |  |
|                            | <b>Post-build time</b> | -- |  |
| <b>Scope / Dependency</b>  | scope: local           |    |  |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00139 :</b>   |    |              |
| <b>Name</b>                             | CsmMacVerifyAlgorithmFamilyCustom                               |    |              |
| <b>Parent Container</b>                 | CsmMacVerifyConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm family used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |                                |    |              |
|---|--------------------------------|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00193 :</b>        |    |              |
| <b>Name</b>                             | CsmMacVerifyAlgorithmKeyLength |    |              |
| <b>Parent Container</b>                 | CsmMacVerifyConfig             |    |              |
| <b>Description</b>                      | Size of the MAC key in bytes   |    |              |
| <b>Multiplicity</b>                     | 1                              |    |              |
| <b>Type</b>                             | EcucIntegerParamDef            |    |              |
| <b>Range</b>                            | 1 .. 4294967295                |    |              |
| <b>Default value</b>                    | --                             |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>        | X  | All Variants |
|   | <b>Link time</b>               | -- |              |
|   | <b>Post-build time</b>         | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>        | X  | All Variants |
|   | <b>Link time</b>               | -- |              |
|   | <b>Post-build time</b>         | -- |              |
| <b>Scope / Dependency</b>               | scope: local                   |    |              |

|                         |   |   |              |
|-------------------------|---|---|--------------|
| <b>SWS Item</b>         | <b>ECUC_Csm_00195 :</b>                                   |   |              |
| <b>Name</b>             | CsmMacVerifyAlgorithmMode                                 |   |              |
| <b>Parent Container</b> | CsmMacVerifyConfig  |   |              |
| <b>Description</b>      | Determines the algorithm mode used for the crypto service |   |              |
| <b>Multiplicity</b>     | 1   |   |              |
| <b>Type</b>             | EcucEnumerationParamDef                                   |   |              |
| <b>Range</b>            | CRYPTO_ALGOMODE_CMAC                                      |   | 0x10         |
|                         | CRYPTO_ALGOMODE_CTRDRBG                                   |   | 0x12         |
|                         | CRYPTO_ALGOMODE_CUSTOM                                    |   | 0xFF         |
|                         | CRYPTO_ALGOMODE_GMAC                                      |   | 0x11         |
|                         | CRYPTO_ALGOMODE_HMAC                                      |   | 0x0f         |
|                         | CRYPTO_ALGOMODE_NOT_SET                                   |   | 0x00         |
|                         | CRYPTO_ALGOMODE_SIPHASH_2_4                               |   | 0x17         |
|                         | CRYPTO_ALGOMODE_SIPHASH_4_8                               |   | 0x18         |
| <b>Multiplicity</b>     | <b>Pre-compile time</b>                                   | X | All Variants |

|                                  |  |    |              |
|----------------------------------|--|----|--------------|
| <b>Configuration Class</b>       | <b>Link time</b>                       | -- |              |
|                                  | <b>Post-build time</b>                 | -- |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>                | X  | All Variants |
|                                  | <b>Link time</b>                       | -- |              |
| <b>Configuration Class</b>       | <b>Post-build time</b>                 | -- |              |
|                                  | <b>Scope / Dependency</b> scope: local |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00194 :</b>                                       |    |              |
| <b>Name</b>                             | CsmMacVerifyAlgorithmModeCustom                               |    |              |
| <b>Parent Container</b>                 | CsmMacVerifyConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00140 :</b>   |      |              |
| <b>Name</b>                             | CsmMacVerifyAlgorithmSecondaryFamily                                  |      |              |
| <b>Parent Container</b>                 | CsmMacVerifyConfig  |      |              |
| <b>Description</b>                      | Determines the secondary algorithm family used for the crypto service |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_CUSTOM   | 0xFF |              |
|   | CRYPTO_ALGOFAM_NOT_SET  | 0x0f |              |
| <b>Default value</b>                    | CRYPTO_ALGOFAM_NOT_SET  |      |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>               | scope: local  |      |              |

|                         |  |  |  |
|-------------------------|--|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00141 :</b>  |  |  |
| <b>Name</b>             | CsmMacVerifyAlgorithmSecondaryFamilyCustom   |  |  |
| <b>Parent Container</b> | CsmMacVerifyConfig   |  |  |
| <b>Description</b>      | This is the second the name of the custom algorithm, if CRYPTO_ALGOFAM_CUSTOM is set as CsmMacVerifyAlgorithmSecondaryFamily |  |  |
| <b>Multiplicity</b>     | 0..1   |  |  |
| <b>Type</b>             | EcucStringParamDef   |  |  |
| <b>Default value</b>    | --   |  |  |
| <b>maxLength</b>        | --   |  |  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>minLength</b>                        | --                      |    |              |
| <b>regularExpression</b>                | --                      |    |              |
| <b>Post-Build Variant Value</b>         | false                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00142 :</b>                                       |    |              |
| <b>Name</b>                             | CsmMacVerifyCompareLength                                     |    |              |
| <b>Parent Container</b>                 | CsmMacVerifyConfig  |    |              |
| <b>Description</b>                      | Size of the input MAC length, that shall be verified, in BITS |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcuIntegerParamDef  |    |              |
| <b>Range</b>                            | 1 .. 4294967295   |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00056 :</b>   |    |              |
| <b>Name</b>                             | CsmMacVerifyDataMaxLength   |    |              |
| <b>Parent Container</b>                 | CsmMacVerifyConfig  |    |              |
| <b>Description</b>                      | Max size of the input data length, for whichs MAC shall be verified, in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcuIntegerParamDef  |    |              |
| <b>Range</b>                            | 1 .. 4294967295   |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

**No Included Containers**

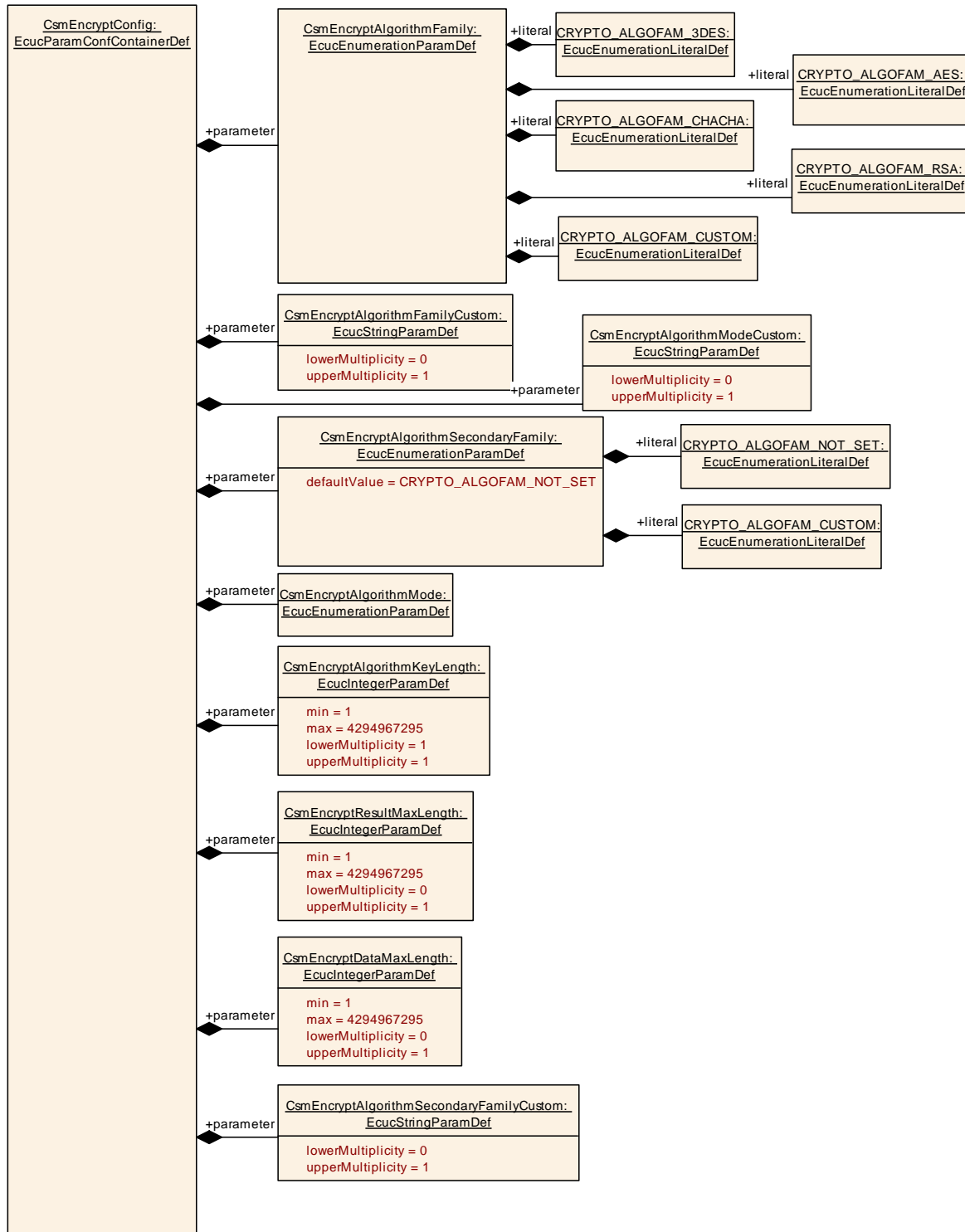


Figure 9-12 CsmEncrypt Layout

10.2.18 CsmEncrypt

|                         |   |
|-------------------------|---|
| <b>SWS Item</b>         | <b>ECUC_Csm_00024 :</b>                 |
| <b>Container Name</b>   | CsmEncrypt                              |
| <b>Parent Container</b> | CsmPrimitives                           |
| <b>Description</b>      | Configurations of Encryption primitives |

|                                 |
|---------------------------------|
| <b>Configuration Parameters</b> |
|---------------------------------|

| <b>Included Containers</b> |                     |  |
|----------------------------|---------------------|--|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>  |
| CsmEncryptConfig           | 1                   | Container for configuration of a CSM encryption interface. The container name serves as a symbolic name for the identifier of an encryption interface. |

### 10.2.19 CsmEncryptConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00057 :</b>  |
| <b>Container Name</b>           | CsmEncryptConfig   |
| <b>Parent Container</b>         | CsmEncrypt   |
| <b>Description</b>              | Container for configuration of a CSM encryption interface. The container name serves as a symbolic name for the identifier of an encryption interface. |
| <b>Configuration Parameters</b> |  |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00182 :</b>   |      |              |
| <b>Name</b>                             | CsmEncryptAlgorithmFamily   |      |              |
| <b>Parent Container</b>                 | CsmEncryptConfig  |      |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_3DES   | 0x13 |              |
|   | CRYPTO_ALGOFAM_AES  | 0x14 |              |
|   | CRYPTO_ALGOFAM_CHACHA   | 0x15 |              |
|   | CRYPTO_ALGOFAM_CUSTOM   | 0xFF |              |
|   | CRYPTO_ALGOFAM_RSA  | 0x16 |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>               | scope: local  |      |              |

|                                 |   |  |  |
|---------------------------------|---|--|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00143 :</b>   |  |  |
| <b>Name</b>                     | CsmEncryptAlgorithmFamilyCustom   |  |  |
| <b>Parent Container</b>         | CsmEncryptConfig  |  |  |
| <b>Description</b>              | This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmEncryptAlgorithmFamily. |  |  |
| <b>Multiplicity</b>             | 0..1  |  |  |
| <b>Type</b>                     | EcucStringParamDef  |  |  |
| <b>Default value</b>            | --  |  |  |
| <b>maxLength</b>                | --  |  |  |
| <b>minLength</b>                | --  |  |  |
| <b>regularExpression</b>        | --  |  |  |
| <b>Post-Build Variant Value</b> | false   |  |  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |                                     |    |              |
|---|-------------------------------------|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00191 :</b>             |    |              |
| <b>Name</b>                             | CsmEncryptAlgorithmKeyLength        |    |              |
| <b>Parent Container</b>                 | CsmEncryptConfig                    |    |              |
| <b>Description</b>                      | Size of the encryption key in bytes |    |              |
| <b>Multiplicity</b>                     | 1                                   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                 |    |              |
| <b>Range</b>                            | 1 .. 4294967295                     |    |              |
| <b>Default value</b>                    | --                                  |    |              |
| <b>Post-Build Variant Value</b>         | false                               |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>             | X  | All Variants |
|   | <b>Link time</b>                    | -- |              |
|   | <b>Post-build time</b>              | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>             | X  | All Variants |
|   | <b>Link time</b>                    | -- |              |
|   | <b>Post-build time</b>              | -- |              |
| <b>Scope / Dependency</b>               | scope: local                        |    |              |

|   |   |       |              |
|---|---|-------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00060 :</b>                                   |       |              |
| <b>Name</b>                             | CsmEncryptAlgorithmMode                                   |       |              |
| <b>Parent Container</b>                 | CsmEncryptConfig  |       |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |       |              |
| <b>Multiplicity</b>                     | 1   |       |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |       |              |
| <b>Range</b>                            | CRYPTO_ALGOMODE_12ROUNDS                                  |       | 0x0d         |
|   | CRYPTO_ALGOMODE_20ROUNDS                                  |       | 0x0e         |
|   | CRYPTO_ALGOMODE_8ROUNDS                                   |       | 0x0c         |
|   | CRYPTO_ALGOMODE_CBC                                       |       | 0x02         |
|   | CRYPTO_ALGOMODE_CFB                                       |       | 0x03         |
|   | CRYPTO_ALGOMODE_CTR                                       |       | 0x05         |
|   | CRYPTO_ALGOMODE_CUSTOM                                    |       | 0xFF         |
|   | CRYPTO_ALGOMODE_ECB                                       |       | 0x01         |
|   | CRYPTO_ALGOMODE_NOT_SET                                   |       | 0x00         |
|   | CRYPTO_ALGOMODE_OFB                                       |       | 0x04         |
|   | CRYPTO_ALGOMODE_RSAES_OAEP                                |       | 0x08         |
|   | CRYPTO_ALGOMODE_RSAES_PKCS1_v1_5                          |       | 0x09         |
|   | CRYPTO_ALGOMODE_XTS                                       |       | 0x06         |
|   | <b>Post-Build Variant Value</b>                           | false |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X     | All Variants |
|   | <b>Link time</b>  | --    |              |
|   | <b>Post-build time</b>                                    | --    |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                   | X     | All Variants |
|   | <b>Link time</b>  | --    |              |
|   | <b>Post-build time</b>                                    | --    |              |
| <b>Scope / Dependency</b>               | scope: local  |       |              |

|                 |                         |  |  |
|-----------------|-------------------------|--|--|
| <b>SWS Item</b> | <b>ECUC_Csm_00153 :</b> |  |  |
|-----------------|-------------------------|--|--|



|   |   |    |              |
|---|---|----|--------------|
| <b>Name</b>                             | CsmEncryptAlgorithmModeCustom                                 |    |              |
| <b>Parent Container</b>                 | CsmEncryptConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00144 :</b>                                     |    |              |
| <b>Name</b>                             | CsmEncryptAlgorithmSecondaryFamily                          |    |              |
| <b>Parent Container</b>                 | CsmEncryptConfig  |    |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                     |    |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_CUSTOM                                       |    | 0xFF         |
|   | CRYPTO_ALGOFAM_NOT_SET                                      |    | 0x00         |
| <b>Default value</b>                    | CRYPTO_ALGOFAM_NOT_SET                                      |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                     | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                      | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                     | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                      | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00190 :</b>   |    |              |
| <b>Name</b>                             | CsmEncryptAlgorithmSecondaryFamilyCustom                                  |    |              |
| <b>Parent Container</b>                 | CsmEncryptConfig  |    |              |
| <b>Description</b>                      | Name of the custom secondary algorithm family used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |



|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00146 :</b>                         |    |              |
| <b>Name</b>                             | CsmEncryptDataMaxLength                         |    |              |
| <b>Parent Container</b>                 | CsmEncryptConfig                                |    |              |
| <b>Description</b>                      | Max size of the input plaintext length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcuIntegerParamDef                              |    |              |
| <b>Range</b>                            | 1 .. 4294967295                                 |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                         | X  | All Variants |
|   | <b>Link time</b>                                | -- |              |
|   | <b>Post-build time</b>                          | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                         | X  | All Variants |
|   | <b>Link time</b>                                | -- |              |
|   | <b>Post-build time</b>                          | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                    |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00147 :</b>                       |    |              |
| <b>Name</b>                             | CsmEncryptResultMaxLength                     |    |              |
| <b>Parent Container</b>                 | CsmEncryptConfig                              |    |              |
| <b>Description</b>                      | Max size of the output cipher length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcuIntegerParamDef                            |    |              |
| <b>Range</b>                            | 1 .. 4294967295                               |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                       | X  | All Variants |
|   | <b>Link time</b>                              | -- |              |
|   | <b>Post-build time</b>                        | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                       | X  | All Variants |
|   | <b>Link time</b>                              | -- |              |
|   | <b>Post-build time</b>                        | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                  |    |              |

**No Included Containers**

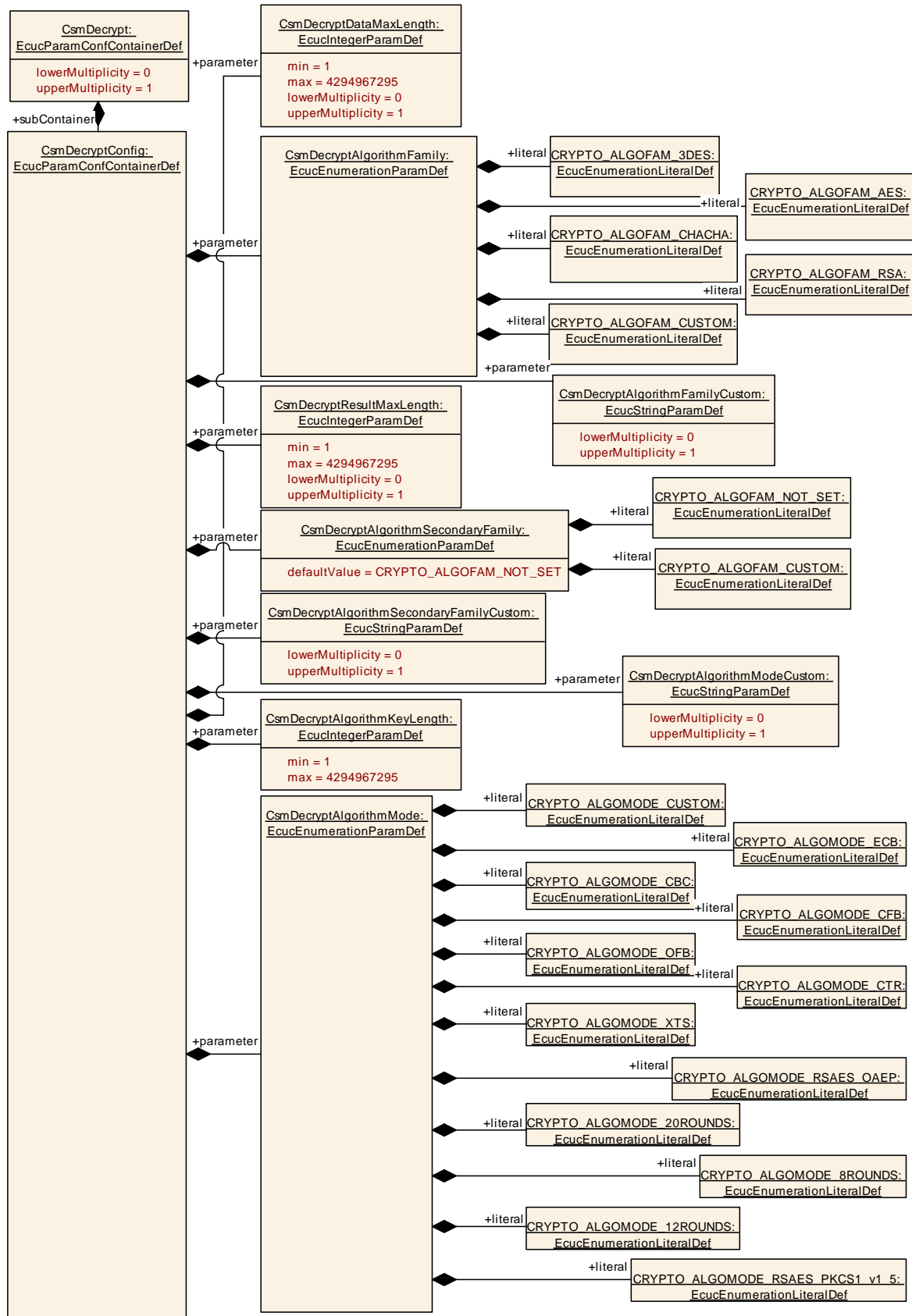


Figure 9-13 CsmDecrypt Layout

### 10.2.20 CsmDecrypt

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00025 :</b>                 |
| <b>Container Name</b>           | CsmDecrypt                              |
| <b>Parent Container</b>         | CsmPrimitives                           |
| <b>Description</b>              | Configurations of Decryption primitives |
| <b>Configuration Parameters</b> |   |

| <b>Included Containers</b> |                     |  |
|----------------------------|---------------------|--|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>  |
| CsmDecryptConfig           | 1                   | Container for configuration of a CSM decryption interface. The container name serves as a symbolic name for the identifier of an decryption interface. |

### 10.2.21 CsmDecryptConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00064 :</b>  |
| <b>Container Name</b>           | CsmDecryptConfig   |
| <b>Parent Container</b>         | CsmDecrypt   |
| <b>Description</b>              | Container for configuration of a CSM decryption interface. The container name serves as a symbolic name for the identifier of an decryption interface. |
| <b>Configuration Parameters</b> |  |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00066 :</b>   |      |              |
| <b>Name</b>                             | CsmDecryptAlgorithmFamily   |      |              |
| <b>Parent Container</b>                 | CsmDecryptConfig  |      |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_3DES   | 0x13 |              |
|   | CRYPTO_ALGOFAM_AES  | 0x14 |              |
|   | CRYPTO_ALGOFAM_CHACHA   | 0x15 |              |
|   | CRYPTO_ALGOFAM_CUSTOM   | 0xFF |              |
|   | CRYPTO_ALGOFAM_RSA  | 0x16 |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>               | scope: local  |      |              |

|                         |   |
|-------------------------|---|
| <b>SWS Item</b>         | <b>ECUC_Csm_00148 :</b>   |
| <b>Name</b>             | CsmDecryptAlgorithmFamilyCustom   |
| <b>Parent Container</b> | CsmDecryptConfig  |
| <b>Description</b>      | Name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmDecryptAlgorithmFamily. |
| <b>Multiplicity</b>     | 0..1  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Type</b>                             | EcucStringParamDef      |    |              |
| <b>Default value</b>                    | --                      |    |              |
| <b>maxLength</b>                        | --                      |    |              |
| <b>minLength</b>                        | --                      |    |              |
| <b>regularExpression</b>                | --                      |    |              |
| <b>Post-Build Variant Value</b>         | false                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |                                     |    |              |
|---|-------------------------------------|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00067 :</b>             |    |              |
| <b>Name</b>                             | CsmDecryptAlgorithmKeyLength        |    |              |
| <b>Parent Container</b>                 | CsmDecryptConfig                    |    |              |
| <b>Description</b>                      | Size of the encryption key in bytes |    |              |
| <b>Multiplicity</b>                     | 1                                   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                 |    |              |
| <b>Range</b>                            | 1 .. 4294967295                     |    |              |
| <b>Default value</b>                    | --                                  |    |              |
| <b>Post-Build Variant Value</b>         | false                               |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>             | X  | All Variants |
|   | <b>Link time</b>                    | -- |              |
|   | <b>Post-build time</b>              | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>             | X  | All Variants |
|   | <b>Link time</b>                    | -- |              |
|   | <b>Post-build time</b>              | -- |              |
| <b>Scope / Dependency</b>               | scope: local                        |    |              |

|   |   |       |              |
|---|---|-------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00068 :</b>                                   |       |              |
| <b>Name</b>                             | CsmDecryptAlgorithmMode                                   |       |              |
| <b>Parent Container</b>                 | CsmDecryptConfig  |       |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |       |              |
| <b>Multiplicity</b>                     | 1   |       |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |       |              |
| <b>Range</b>                            | CRYPTO_ALGOMODE_12ROUNDS                                  |       | 0x0d         |
|   | CRYPTO_ALGOMODE_20ROUNDS                                  |       | 0x0e         |
|   | CRYPTO_ALGOMODE_8ROUNDS                                   |       | 0x0c         |
|   | CRYPTO_ALGOMODE_CBC                                       |       | 0x02         |
|   | CRYPTO_ALGOMODE_CFB                                       |       | 0x03         |
|   | CRYPTO_ALGOMODE_CTR                                       |       | 0x05         |
|   | CRYPTO_ALGOMODE_CUSTOM                                    |       | 0xFF         |
|   | CRYPTO_ALGOMODE_ECB                                       |       | 0x01         |
|   | CRYPTO_ALGOMODE_OFB                                       |       | 0x04         |
|   | CRYPTO_ALGOMODE_RSAES_OAEP                                |       | 0x08         |
|   | CRYPTO_ALGOMODE_RSAES_PKCS1_v1_5                          |       | 0x09         |
|   | CRYPTO_ALGOMODE_XTS                                       |       | 0x06         |
|   | <b>Post-Build Variant Value</b>                           | false |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X     | All Variants |
|   | <b>Link time</b>  | --    |              |
|   | <b>Post-build time</b>                                    | --    |              |
| <b>Value</b>                            | <b>Pre-compile time</b>                                   | X     | All Variants |

|                            |                        |    |  |
|----------------------------|------------------------|----|--|
| <b>Configuration Class</b> | <b>Link time</b>       | -- |  |
|                            | <b>Post-build time</b> | -- |  |
| <b>Scope / Dependency</b>  | scope: local           |    |  |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00152 :</b>                                       |    |              |
| <b>Name</b>                             | CsmDecryptAlgorithmModeCustom                                 |    |              |
| <b>Parent Container</b>                 | CsmDecryptConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00149 :</b>   |    |              |
| <b>Name</b>                             | CsmDecryptAlgorithmSecondaryFamily                                    |    |              |
| <b>Parent Container</b>                 | CsmDecryptConfig  |    |              |
| <b>Description</b>                      | Determines the secondary algorithm family used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |    |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_CUSTOM   |    | 0xFF         |
|   | CRYPTO_ALGOFAM_NOT_SET  |    | 0x00         |
| <b>Default value</b>                    | CRYPTO_ALGOFAM_NOT_SET  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                                   |   |   |              |
|-----------------------------------|---|---|--------------|
| <b>SWS Item</b>                   | <b>ECUC_Csm_00150 :</b>   |   |              |
| <b>Name</b>                       | CsmDecryptAlgorithmSecondaryFamilyCustom                                  |   |              |
| <b>Parent Container</b>           | CsmDecryptConfig  |   |              |
| <b>Description</b>                | Name of the custom secondary algorithm family used for the crypto service |   |              |
| <b>Multiplicity</b>               | 0..1  |   |              |
| <b>Type</b>                       | EcucStringParamDef  |   |              |
| <b>Default value</b>              | --  |   |              |
| <b>maxLength</b>                  | --  |   |              |
| <b>minLength</b>                  | --  |   |              |
| <b>regularExpression</b>          | --  |   |              |
| <b>Post-Build Variant Value</b>   | false   |   |              |
| <b>Multiplicity Configuration</b> | <b>Pre-compile time</b>   | X | All Variants |

|                                  |                         |    |              |
|----------------------------------|-------------------------|----|--------------|
| <b>Class</b>                     | <b>Link time</b>        | -- |              |
|                                  | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|                                  | <b>Link time</b>        | -- |              |
|                                  | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>        | scope: local            |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00154 :</b>                          |    |              |
| <b>Name</b>                             | CsmDecryptDataMaxLength                          |    |              |
| <b>Parent Container</b>                 | CsmDecryptConfig                                 |    |              |
| <b>Description</b>                      | Max size of the input ciphertext length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                              |    |              |
| <b>Range</b>                            | 1 .. 4294967295                                  |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                          | X  | All Variants |
|   | <b>Link time</b>                                 | -- |              |
|   | <b>Post-build time</b>                           | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                          | X  | All Variants |
|   | <b>Link time</b>                                 | -- |              |
|   | <b>Post-build time</b>                           | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                     |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00155 :</b>                          |    |              |
| <b>Name</b>                             | CsmDecryptResultMaxLength                        |    |              |
| <b>Parent Container</b>                 | CsmDecryptConfig                                 |    |              |
| <b>Description</b>                      | Max size of the output plaintext length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                              |    |              |
| <b>Range</b>                            | 1 .. 4294967295                                  |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                          | X  | All Variants |
|   | <b>Link time</b>                                 | -- |              |
|   | <b>Post-build time</b>                           | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                          | X  | All Variants |
|   | <b>Link time</b>                                 | -- |              |
|   | <b>Post-build time</b>                           | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                     |    |              |

|                               |
|-------------------------------|
| <b>No Included Containers</b> |
|-------------------------------|

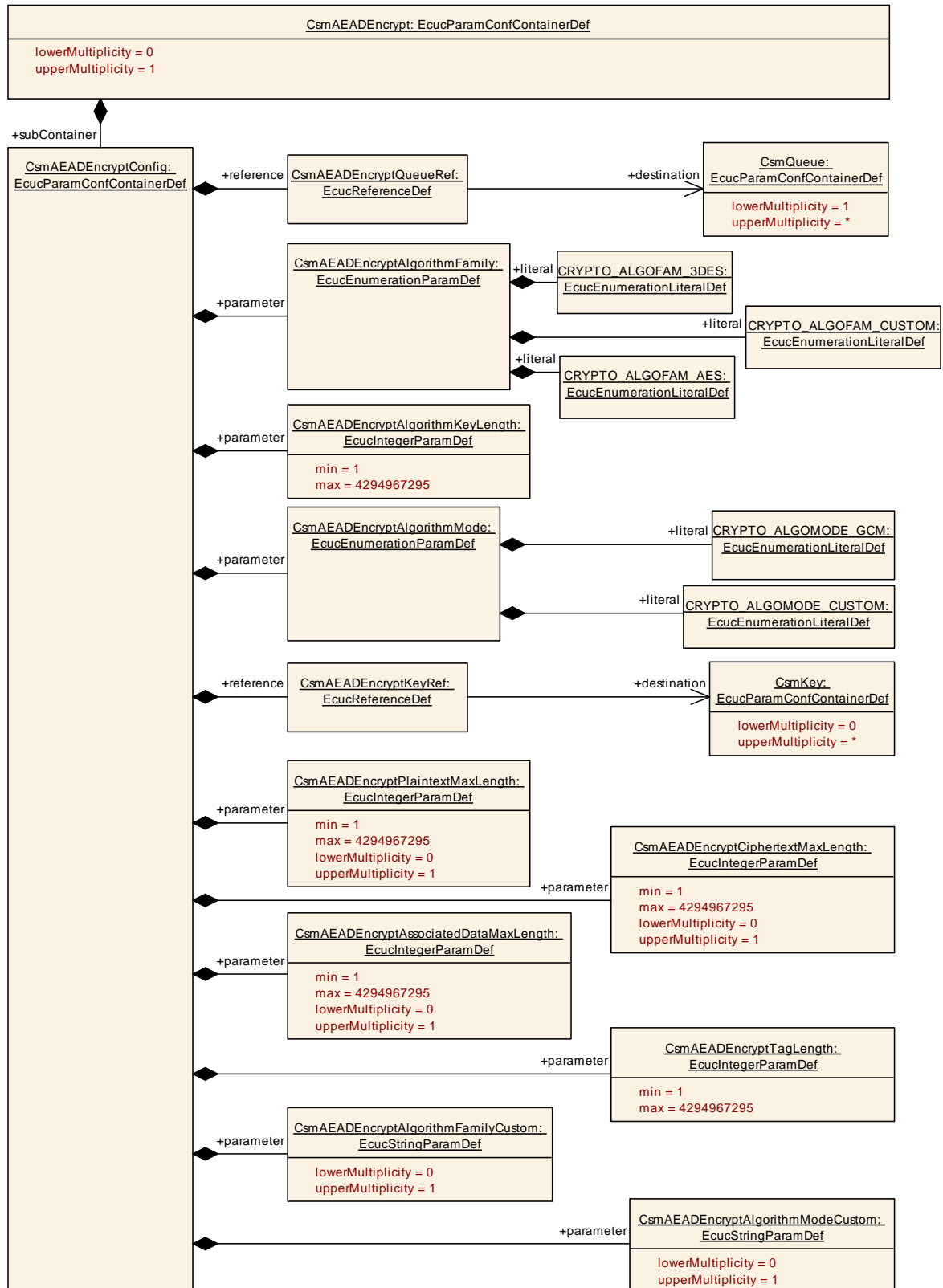


Figure 9-14 CsmAEADEncrypt Layout

## 10.2.22 CsmAEADEncrypt

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00026 :</b>                     |
| <b>Container Name</b>           | CsmAEADEncrypt                              |
| <b>Parent Container</b>         | CsmPrimitives                               |
| <b>Description</b>              | Configuration of AEAD encryption primitives |
| <b>Configuration Parameters</b> |   |

| <b>Included Containers</b> |                     |  |
|----------------------------|---------------------|--|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>  |
| CsmAEADEncryptConfig       | 1                   | Container for configuration of a CSM encryption interface. The container name serves as a symbolic name for the identifier of an encryption interface. |

## 10.2.23 CsmAEADEncryptConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00072 :</b>  |
| <b>Container Name</b>           | CsmAEADEncryptConfig   |
| <b>Parent Container</b>         | CsmAEADEncrypt   |
| <b>Description</b>              | Container for configuration of a CSM encryption interface. The container name serves as a symbolic name for the identifier of an encryption interface. |
| <b>Configuration Parameters</b> |  |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00074 :</b>   |      |              |
| <b>Name</b>                             | CsmAEADEncryptAlgorithmFamily   |      |              |
| <b>Parent Container</b>                 | CsmAEADEncryptConfig  |      |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_3DES   | 0x13 |              |
|   | CRYPTO_ALGOFAM_AES  | 0x14 |              |
|   | CRYPTO_ALGOFAM_CUSTOM   | 0xFF |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>               | scope: local  |      |              |

|                         |   |
|-------------------------|---|
| <b>SWS Item</b>         | <b>ECUC_Csm_00184 :</b>   |
| <b>Name</b>             | CsmAEADEncryptAlgorithmFamilyCustom   |
| <b>Parent Container</b> | CsmAEADEncryptConfig  |
| <b>Description</b>      | This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmAEADEncryptAlgorithmFamily. |
| <b>Multiplicity</b>     | 0..1  |
| <b>Type</b>             | EcucStringParamDef  |



|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Default value</b>                    | --                      |    |              |
| <b>maxLength</b>                        | --                      |    |              |
| <b>minLength</b>                        | --                      |    |              |
| <b>regularExpression</b>                | --                      |    |              |
| <b>Post-Build Variant Value</b>         | false                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00075 :</b>                  |    |              |
| <b>Name</b>                             | CsmAEADEncryptAlgorithmKeyLength         |    |              |
| <b>Parent Container</b>                 | CsmAEADEncryptConfig                     |    |              |
| <b>Description</b>                      | Size of the AEAD encryption key in bytes |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                      |    |              |
| <b>Range</b>                            | 1 .. 4294967295                          |    |              |
| <b>Default value</b>                    | --                                       |    |              |
| <b>Post-Build Variant Value</b>         | false                                    |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                  | X  | All Variants |
|   | <b>Link time</b>                         | -- |              |
|   | <b>Post-build time</b>                   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                  | X  | All Variants |
|   | <b>Link time</b>                         | -- |              |
|   | <b>Post-build time</b>                   | -- |              |
| <b>Scope / Dependency</b>               | scope: local                             |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00076 :</b>                                   |    |              |
| <b>Name</b>                             | CsmAEADEncryptAlgorithmMode                               |    |              |
| <b>Parent Container</b>                 | CsmAEADEncryptConfig                                      |    |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |    |              |
| <b>Range</b>                            | CRYPTO_ALGOMODE_CUSTOM                                    |    | 0xFF         |
|   | CRYPTO_ALGOMODE_GCM                                       |    | 0x07         |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                         |   |  |  |
|-------------------------|---|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00187 :</b>                                       |  |  |
| <b>Name</b>             | CsmAEADEncryptAlgorithmModeCustom                             |  |  |
| <b>Parent Container</b> | CsmAEADEncryptConfig  |  |  |
| <b>Description</b>      | Name of the custom algorithm mode used for the crypto service |  |  |
| <b>Multiplicity</b>     | 0..1  |  |  |
| <b>Type</b>             | EcucStringParamDef  |  |  |
| <b>Default value</b>    | --  |  |  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>maxLength</b>                        | --                      |    |              |
| <b>minLength</b>                        | --                      |    |              |
| <b>regularExpression</b>                | --                      |    |              |
| <b>Post-Build Variant Value</b>         | false                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00159 :</b>                               |    |              |
| <b>Name</b>                             | CsmAEADEncryptAssociatedDataMaxLength                 |    |              |
| <b>Parent Container</b>                 | CsmAEADEncryptConfig                                  |    |              |
| <b>Description</b>                      | Max size of the input associated data length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                                   |    |              |
| <b>Range</b>                            | 1 .. 4294967295                                       |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                               | X  | All Variants |
|   | <b>Link time</b>                                      | -- |              |
|   | <b>Post-build time</b>                                | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                               | X  | All Variants |
|   | <b>Link time</b>                                      | -- |              |
|   | <b>Post-build time</b>                                | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00160 :</b>                           |    |              |
| <b>Name</b>                             | CsmAEADEncryptCiphertextMaxLength                 |    |              |
| <b>Parent Container</b>                 | CsmAEADEncryptConfig                              |    |              |
| <b>Description</b>                      | Max size of the output ciphertext length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                               |    |              |
| <b>Range</b>                            | 1 .. 4294967295                                   |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                           | X  | All Variants |
|   | <b>Link time</b>                                  | -- |              |
|   | <b>Post-build time</b>                            | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                           | X  | All Variants |
|   | <b>Link time</b>                                  | -- |              |
|   | <b>Post-build time</b>                            | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                      |    |              |

|                                 |   |  |  |
|---------------------------------|---|--|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00158 :</b>                         |  |  |
| <b>Name</b>                     | CsmAEADEncryptPlaintextMaxLength                |  |  |
| <b>Parent Container</b>         | CsmAEADEncryptConfig                            |  |  |
| <b>Description</b>              | Max size of the input plaintext length in bytes |  |  |
| <b>Multiplicity</b>             | 0..1  |  |  |
| <b>Type</b>                     | EcucIntegerParamDef                             |  |  |
| <b>Range</b>                    | 1 .. 4294967295                                 |  |  |
| <b>Default value</b>            | --  |  |  |
| <b>Post-Build Variant Value</b> | false   |  |  |

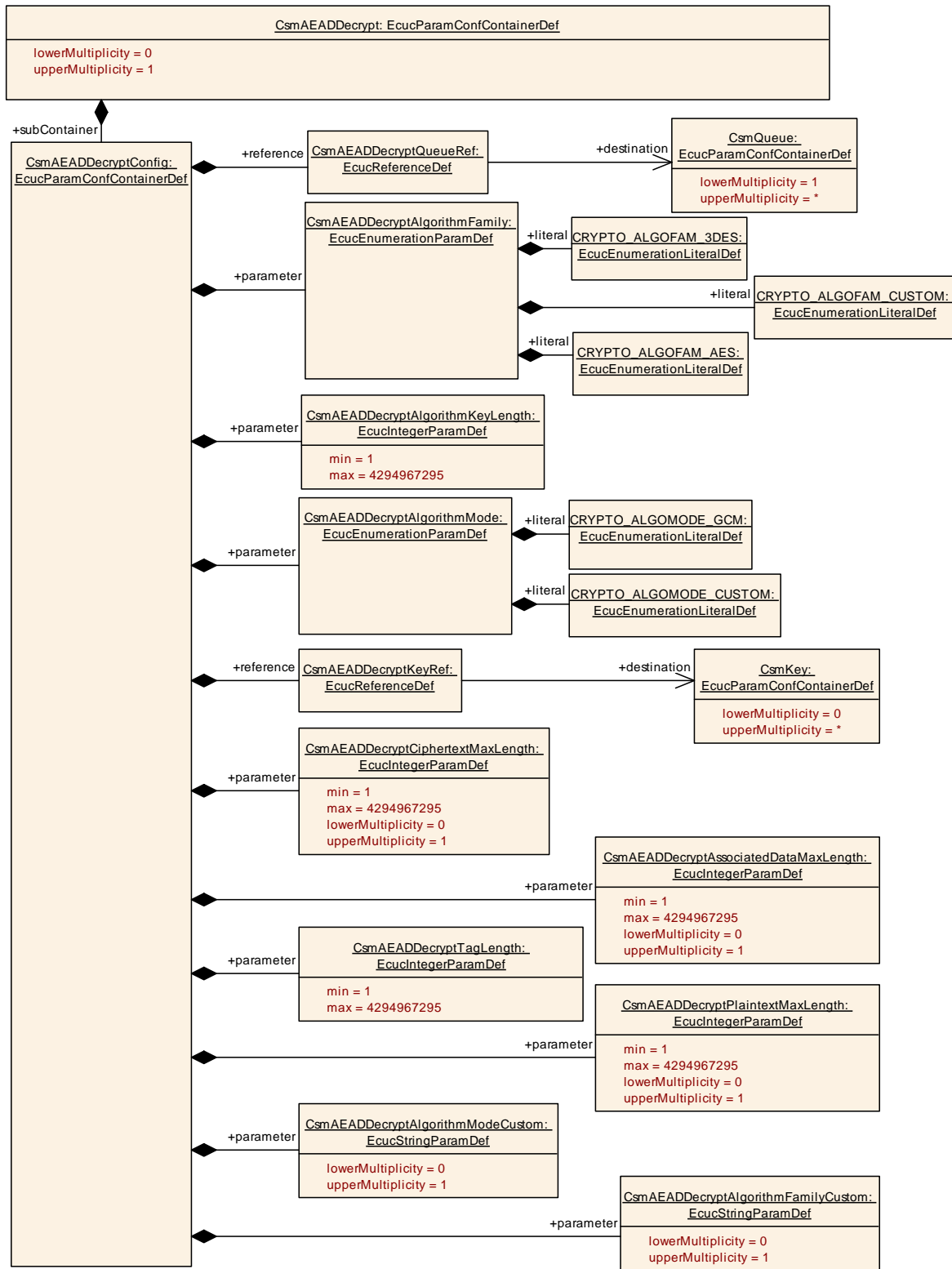
|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00161 :</b>                |    |              |
| <b>Name</b>                             | CsmAEADEncryptTagLength                |    |              |
| <b>Parent Container</b>                 | CsmAEADEncryptConfig                   |    |              |
| <b>Description</b>                      | Size of the output Tag length in bytes |    |              |
| <b>Multiplicity</b>                     | 1                                      |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                    |    |              |
| <b>Range</b>                            | 1 .. 4294967295                        |    |              |
| <b>Default value</b>                    | --                                     |    |              |
| <b>Post-Build Variant Value</b>         | false                                  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                | X  | All Variants |
|   | <b>Link time</b>                       | -- |              |
|   | <b>Post-build time</b>                 | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                | X  | All Variants |
|   | <b>Link time</b>                       | -- |              |
|   | <b>Post-build time</b>                 | -- |              |
| <b>Scope / Dependency</b>               | scope: local                           |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00157 :</b>  |    |              |
| <b>Name</b>                             | CsmAEADEncryptKeyRef   |    |              |
| <b>Parent Container</b>                 | CsmAEADEncryptConfig   |    |              |
| <b>Description</b>                      | This parameter refers to the key used for that encryption primitive. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | Reference to [ CsmKey ]  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00156 :</b>  |    |              |
| <b>Name</b>                             | CsmAEADEncryptQueueRef   |    |              |
| <b>Parent Container</b>                 | CsmAEADEncryptConfig   |    |              |
| <b>Description</b>                      | This parameter refers to the queue used for that encryption primitive. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | Reference to [ CsmQueue ]  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

**No Included Containers**



**Figure 9-15 CsmAEADDecrypt Layout**

## 10.2.24 CsmAEADDecrypt

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00027 :</b>                     |
| <b>Container Name</b>           | CsmAEADDecrypt                              |
| <b>Parent Container</b>         | CsmPrimitives                               |
| <b>Description</b>              | Configuration of AEAD decryption primitives |
| <b>Configuration Parameters</b> |   |

| <b>Included Containers</b> |                     |  |
|----------------------------|---------------------|--|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>  |
| CsmAEADDecryptConfig       | 1                   | Container for configuration of a CSM decryption interface. The container name serves as a symbolic name for the identifier of an decryption interface. |

## 10.2.25 CsmAEADDecryptConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00080 :</b>  |
| <b>Container Name</b>           | CsmAEADDecryptConfig   |
| <b>Parent Container</b>         | CsmAEADDecrypt   |
| <b>Description</b>              | Container for configuration of a CSM decryption interface. The container name serves as a symbolic name for the identifier of an decryption interface. |
| <b>Configuration Parameters</b> |  |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00082 :</b>   |      |              |
| <b>Name</b>                             | CsmAEADDecryptAlgorithmFamily   |      |              |
| <b>Parent Container</b>                 | CsmAEADDecryptConfig  |      |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_3DES   | 0x13 |              |
|   | CRYPTO_ALGOFAM_AES  | 0x14 |              |
|   | CRYPTO_ALGOFAM_CUSTOM   | 0xFF |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>               | scope: local  |      |              |

|                         |   |
|-------------------------|---|
| <b>SWS Item</b>         | <b>ECUC_Csm_00185 :</b>   |
| <b>Name</b>             | CsmAEADDecryptAlgorithmFamilyCustom   |
| <b>Parent Container</b> | CsmAEADDecryptConfig  |
| <b>Description</b>      | This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmAEADDecryptAlgorithmFamily. |
| <b>Multiplicity</b>     | 0..1  |
| <b>Type</b>             | EcucStringParamDef  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Default value</b>                    | --                      |    |              |
| <b>maxLength</b>                        | --                      |    |              |
| <b>minLength</b>                        | --                      |    |              |
| <b>regularExpression</b>                | --                      |    |              |
| <b>Post-Build Variant Value</b>         | false                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00083 :</b>                  |    |              |
| <b>Name</b>                             | CsmAEADDecryptAlgorithmKeyLength         |    |              |
| <b>Parent Container</b>                 | CsmAEADDecryptConfig                     |    |              |
| <b>Description</b>                      | Size of the AEAD decryption key in bytes |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                      |    |              |
| <b>Range</b>                            | 1 .. 4294967295                          |    |              |
| <b>Default value</b>                    | --                                       |    |              |
| <b>Post-Build Variant Value</b>         | false                                    |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                  | X  | All Variants |
|   | <b>Link time</b>                         | -- |              |
|   | <b>Post-build time</b>                   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                  | X  | All Variants |
|   | <b>Link time</b>                         | -- |              |
|   | <b>Post-build time</b>                   | -- |              |
| <b>Scope / Dependency</b>               | scope: local                             |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00084 :</b>                                   |    |              |
| <b>Name</b>                             | CsmAEADDecryptAlgorithmMode                               |    |              |
| <b>Parent Container</b>                 | CsmAEADDecryptConfig                                      |    |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |    |              |
| <b>Range</b>                            | CRYPTO_ALGOMODE_CUSTOM                                    |    | 0xFF         |
|   | CRYPTO_ALGOMODE_GCM                                       |    | 0x07         |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                         |   |  |  |
|-------------------------|---|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00186 :</b>                                       |  |  |
| <b>Name</b>             | CsmAEADDecryptAlgorithmModeCustom                             |  |  |
| <b>Parent Container</b> | CsmAEADDecryptConfig  |  |  |
| <b>Description</b>      | Name of the custom algorithm mode used for the crypto service |  |  |
| <b>Multiplicity</b>     | 0..1  |  |  |
| <b>Type</b>             | EcucStringParamDef  |  |  |
| <b>Default value</b>    | --  |  |  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>maxLength</b>                        | --                      |    |              |
| <b>minLength</b>                        | --                      |    |              |
| <b>regularExpression</b>                | --                      |    |              |
| <b>Post-Build Variant Value</b>         | false                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00163 :</b>                               |    |              |
| <b>Name</b>                             | CsmAEADDecryptAssociatedDataMaxLength                 |    |              |
| <b>Parent Container</b>                 | CsmAEADDecryptConfig                                  |    |              |
| <b>Description</b>                      | Max size of the input associated data length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                                   |    |              |
| <b>Range</b>                            | 1 .. 4294967295                                       |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                               | X  | All Variants |
|   | <b>Link time</b>                                      | -- |              |
|   | <b>Post-build time</b>                                | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                               | X  | All Variants |
|   | <b>Link time</b>                                      | -- |              |
|   | <b>Post-build time</b>                                | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00162 :</b>                   |    |              |
| <b>Name</b>                             | CsmAEADDecryptCiphertextMaxLength         |    |              |
| <b>Parent Container</b>                 | CsmAEADDecryptConfig                      |    |              |
| <b>Description</b>                      | Max size of the input ciphertext in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1                                      |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                       |    |              |
| <b>Range</b>                            | 1 .. 4294967295                           |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false                                     |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                   | X  | All Variants |
|   | <b>Link time</b>                          | -- |              |
|   | <b>Post-build time</b>                    | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                   | X  | All Variants |
|   | <b>Link time</b>                          | -- |              |
|   | <b>Post-build time</b>                    | -- |              |
| <b>Scope / Dependency</b>               | scope: local                              |    |              |

|                                 |  |  |  |
|---------------------------------|--|--|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00165 :</b>                      |  |  |
| <b>Name</b>                     | CsmAEADDecryptPlaintextMaxLength             |  |  |
| <b>Parent Container</b>         | CsmAEADDecryptConfig                         |  |  |
| <b>Description</b>              | Size of the output plaintext length in bytes |  |  |
| <b>Multiplicity</b>             | 0..1   |  |  |
| <b>Type</b>                     | EcucIntegerParamDef                          |  |  |
| <b>Range</b>                    | 1 .. 4294967295                              |  |  |
| <b>Default value</b>            | --   |  |  |
| <b>Post-Build Variant Value</b> | false  |  |  |



|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

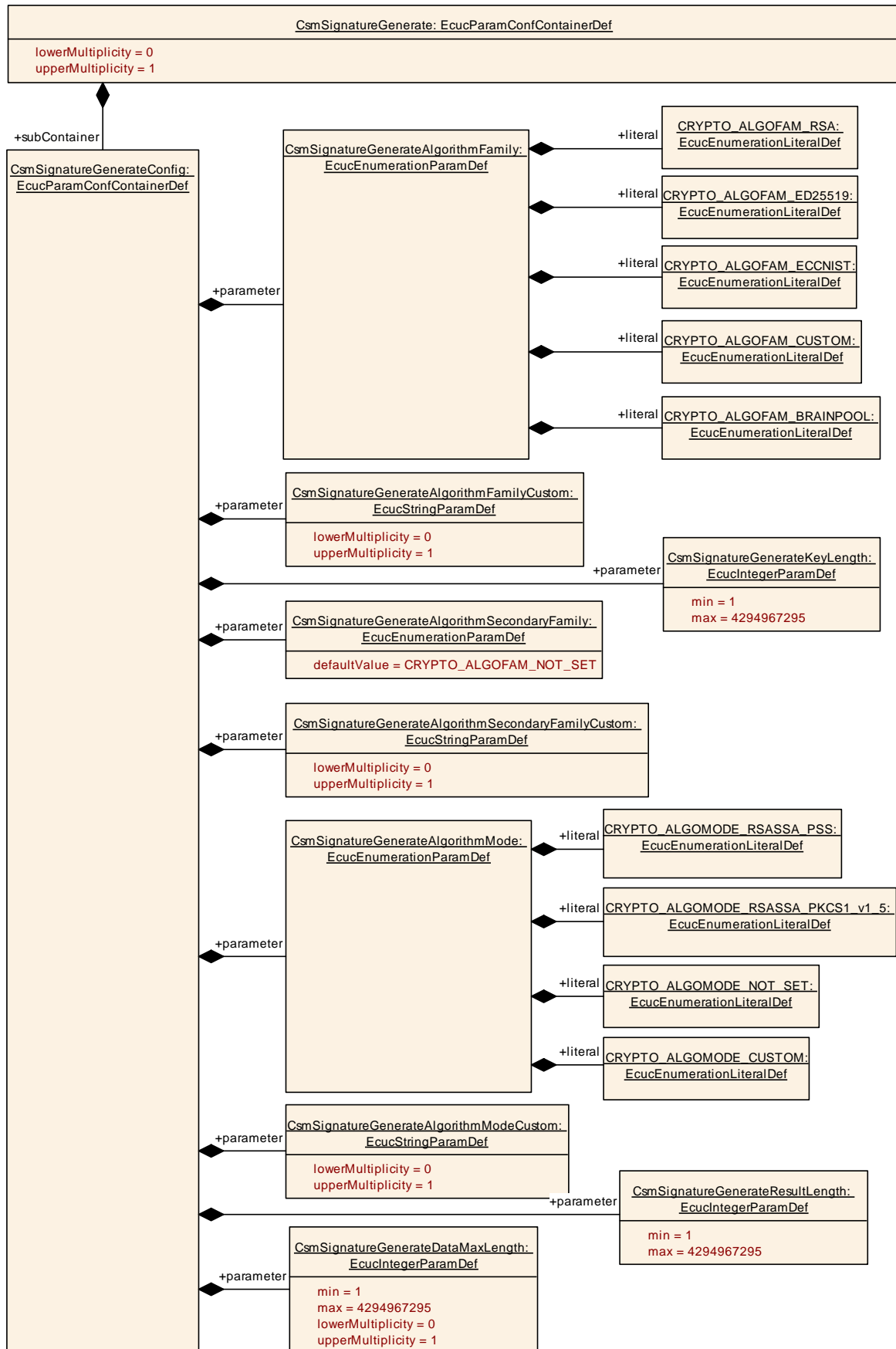
|   |                                      |    |              |
|---|--------------------------------------|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00164 :</b>              |    |              |
| <b>Name</b>                             | CsmAEADDecryptTagLength              |    |              |
| <b>Parent Container</b>                 | CsmAEADDecryptConfig                 |    |              |
| <b>Description</b>                      | Size of the input Tag length in BITS |    |              |
| <b>Multiplicity</b>                     | 1                                    |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                  |    |              |
| <b>Range</b>                            | 1 .. 4294967295                      |    |              |
| <b>Default value</b>                    | --                                   |    |              |
| <b>Post-Build Variant Value</b>         | false                                |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>              | X  | All Variants |
|   | <b>Link time</b>                     | -- |              |
|   | <b>Post-build time</b>               | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>              | X  | All Variants |
|   | <b>Link time</b>                     | -- |              |
|   | <b>Post-build time</b>               | -- |              |
| <b>Scope / Dependency</b>               | scope: local                         |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00086 :</b>  |    |              |
| <b>Name</b>                             | CsmAEADDecryptKeyRef   |    |              |
| <b>Parent Container</b>                 | CsmAEADDecryptConfig   |    |              |
| <b>Description</b>                      | This parameter refers to the key used for that decryption primitive. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | Reference to [ CsmKey ]  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00081 :</b>  |    |              |
| <b>Name</b>                             | CsmAEADDecryptQueueRef   |    |              |
| <b>Parent Container</b>                 | CsmAEADDecryptConfig   |    |              |
| <b>Description</b>                      | This parameter refers to the queue used for that decryption primitive. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | Reference to [ CsmQueue ]  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |



*No Included Containers*



**Figure 9-16 CsmSignatureGenerate Layout**

### 10.2.26 CsmSignatureGenerate

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00028 :</b>                        |
| <b>Container Name</b>           | CsmSignatureGenerate                           |
| <b>Parent Container</b>         | CsmPrimitives                                  |
| <b>Description</b>              | Configurations of SignatureGenerate primitives |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmSignatureGenerateConfig | 1                   | Container for configuration of a CSM signature generation interface. The container name serves as a symbolic name for the identifier of signature generation interface. |

### 10.2.27 CsmSignatureGenerateConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00087 :</b>   |
| <b>Container Name</b>           | CsmSignatureGenerateConfig  |
| <b>Parent Container</b>         | CsmSignatureGenerate  |
| <b>Description</b>              | Container for configuration of a CSM signature generation interface. The container name serves as a symbolic name for the identifier of signature generation interface. |
| <b>Configuration Parameters</b> |   |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00089 :</b>   |    |              |
| <b>Name</b>                             | CsmSignatureGenerateAlgorithmFamily   |    |              |
| <b>Parent Container</b>                 | CsmSignatureGenerateConfig  |    |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |    |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_BRAINPOOL  |    | 0x15         |
|   | CRYPTO_ALGOFAM_CUSTOM   |    | 0xFF         |
|   | CRYPTO_ALGOFAM_ECCNIST  |    | 0x16         |
|   | CRYPTO_ALGOFAM_ED25519  |    | 0x14         |
|   | CRYPTO_ALGOFAM_RSA  |    | 0x13         |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                         |   |
|-------------------------|---|
| <b>SWS Item</b>         | <b>ECUC_Csm_00166 :</b>                   |
| <b>Name</b>             | CsmSignatureGenerateAlgorithmFamilyCustom |
| <b>Parent Container</b> | CsmSignatureGenerateConfig                |

|   |   |    |              |
|---|---|----|--------------|
| <b>Description</b>                      | Name of the custom algorithm family used for the crypto service.<br>This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmSignatureGenerateAlgorithmFamily. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00091 :</b>                                   |    |              |
| <b>Name</b>                             | CsmSignatureGenerateAlgorithmMode                         |    |              |
| <b>Parent Container</b>                 | CsmSignatureGenerateConfig                                |    |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |    |              |
| <b>Range</b>                            | CRYPTO_ALGOMODE_CUSTOM                                    |    | 0xFF         |
|   | CRYPTO_ALGOMODE_NOT_SET                                   |    | 0x00         |
|   | CRYPTO_ALGOMODE_RSASSA_PKCS1_v1_5                         |    | 0x0b         |
|   | CRYPTO_ALGOMODE_RSASSA_PSS                                |    | 0x0a         |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00168 :</b>                                       |    |              |
| <b>Name</b>                             | CsmSignatureGenerateAlgorithmModeCustom                       |    |              |
| <b>Parent Container</b>                 | CsmSignatureGenerateConfig                                    |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |

|                           |                        |    |  |
|---------------------------|------------------------|----|--|
|                           | <b>Post-build time</b> | -- |  |
| <b>Scope / Dependency</b> | scope: local           |    |  |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00183 :</b>                                   |      |              |
| <b>Name</b>                             | CsmSignatureGenerateAlgorithmSecondaryFamily              |      |              |
| <b>Parent Container</b>                 | CsmSignatureGenerateConfig                                |      |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_BLAKE_1_256                                |      | 0x0F         |
|   | CRYPTO_ALGOFAM_BLAKE_1_512                                |      | 0x10         |
|   | CRYPTO_ALGOFAM_BLAKE_2s_256                               |      | 0x11         |
|   | CRYPTO_ALGOFAM_BLAKE_2s_512                               |      | 0x12         |
|   | CRYPTO_ALGOFAM_CUSTOM                                     |      | 0xFF         |
|   | CRYPTO_ALGOFAM_NOT_SET                                    |      | 0x00         |
|   | CRYPTO_ALGOFAM_RIPEMD160                                  |      | 0x0E         |
|   | CRYPTO_ALGOFAM_SHA1                                       |      | 0x01         |
|   | CRYPTO_ALGOFAM_SHA2_224                                   |      | 0x02         |
|   | CRYPTO_ALGOFAM_SHA2_256                                   |      | 0x03         |
|   | CRYPTO_ALGOFAM_SHA2_384                                   |      | 0x04         |
|   | CRYPTO_ALGOFAM_SHA2_512                                   |      | 0x05         |
|   | CRYPTO_ALGOFAM_SHA2_512_224                               |      | 0x06         |
|   | CRYPTO_ALGOFAM_SHA2_512_256                               |      | 0x07         |
|   | CRYPTO_ALGOFAM_SHA3_224                                   |      | 0x08         |
|   | CRYPTO_ALGOFAM_SHA3_256                                   |      | 0x09         |
|   | CRYPTO_ALGOFAM_SHA3_384                                   |      | 0x0A         |
|   | CRYPTO_ALGOFAM_SHA3_512                                   |      | 0x0B         |
|   | CRYPTO_ALGOFAM_SHAKE128                                   |      | 0x0C         |
| CRYPTO_ALGOFAM_SHAKE256                 |   | 0x0D |              |
| <b>Default value</b>                    | CRYPTO_ALGOFAM_NOT_SET                                    |      |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>                                    | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>                                    | --   |              |
| <b>Scope / Dependency</b>               | scope: local  |      |              |

|                                   |   |   |              |
|-----------------------------------|---|---|--------------|
| <b>SWS Item</b>                   | <b>ECUC_Csm_00167 :</b>   |   |              |
| <b>Name</b>                       | CsmSignatureGenerateAlgorithmSecondaryFamilyCustom  |   |              |
| <b>Parent Container</b>           | CsmSignatureGenerateConfig  |   |              |
| <b>Description</b>                | Name of the custom secondary algorithm family used for the crypto service. This is the second name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is set as CsmSignatureGenerateAlgorithmSecondaryFamily. |   |              |
| <b>Multiplicity</b>               | 0..1  |   |              |
| <b>Type</b>                       | EcucStringParamDef  |   |              |
| <b>Default value</b>              | --  |   |              |
| <b>maxLength</b>                  | --  |   |              |
| <b>minLength</b>                  | --  |   |              |
| <b>regularExpression</b>          | --  |   |              |
| <b>Post-Build Variant Value</b>   | false   |   |              |
| <b>Multiplicity Configuration</b> | <b>Pre-compile time</b>   | X | All Variants |

|                                  |                         |    |              |
|----------------------------------|-------------------------|----|--------------|
| <b>Class</b>                     | <b>Link time</b>        | -- |              |
|                                  | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|                                  | <b>Link time</b>        | -- |              |
|                                  | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>        | scope: local            |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00169 :</b>                |    |              |
| <b>Name</b>                             | CsmSignatureGenerateDataMaxLength      |    |              |
| <b>Parent Container</b>                 | CsmSignatureGenerateConfig             |    |              |
| <b>Description</b>                      | Size of the input data length in bytes |    |              |
| <b>Multiplicity</b>                     | 0..1                                   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                    |    |              |
| <b>Range</b>                            | 1 .. 4294967295                        |    |              |
| <b>Default value</b>                    | --                                     |    |              |
| <b>Post-Build Variant Value</b>         | false                                  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                | X  | All Variants |
|   | <b>Link time</b>                       | -- |              |
|   | <b>Post-build time</b>                 | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                | X  | All Variants |
|   | <b>Link time</b>                       | -- |              |
|   | <b>Post-build time</b>                 | -- |              |
| <b>Scope / Dependency</b>               | scope: local                           |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00090 :</b>                     |    |              |
| <b>Name</b>                             | CsmSignatureGenerateKeyLength               |    |              |
| <b>Parent Container</b>                 | CsmSignatureGenerateConfig                  |    |              |
| <b>Description</b>                      | Size of the signature generate key in bytes |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                         |    |              |
| <b>Range</b>                            | 1 .. 4294967295                             |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false                                       |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|   | <b>Link time</b>                            | -- |              |
|   | <b>Post-build time</b>                      | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                     | X  | All Variants |
|   | <b>Link time</b>                            | -- |              |
|   | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00170 :</b>                      |    |              |
| <b>Name</b>                             | CsmSignatureGenerateResultLength             |    |              |
| <b>Parent Container</b>                 | CsmSignatureGenerateConfig                   |    |              |
| <b>Description</b>                      | Size of the output signature length in bytes |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                          |    |              |
| <b>Range</b>                            | 1 .. 4294967295                              |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                      | X  | All Variants |
|   | <b>Link time</b>                             | -- |              |
|   | <b>Post-build time</b>                       | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                      | X  | All Variants |
|   | <b>Link time</b>                             | -- |              |

|                               |                        |    |  |
|-------------------------------|------------------------|----|--|
|                               | <i>Post-build time</i> | -- |  |
| <i>Scope / Dependency</i>     | scope: local           |    |  |
| <b>No Included Containers</b> |                        |    |  |

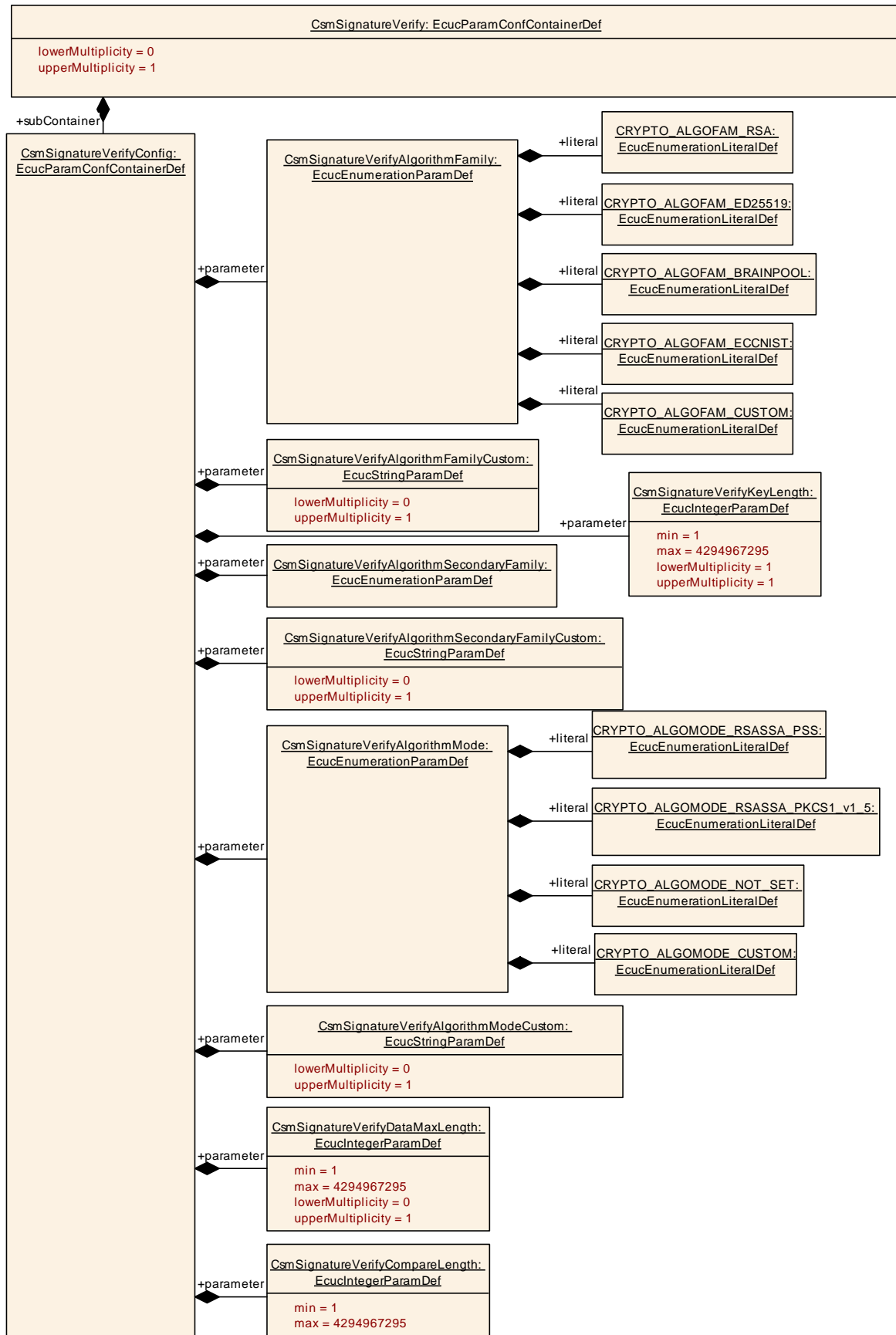


Figure 9-17 CsmSignatureVerify Layout



## 10.2.28 CsmSignatureVerify

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00029 :</b>                      |
| <b>Container Name</b>           | CsmSignatureVerify                           |
| <b>Parent Container</b>         | CsmPrimitives                                |
| <b>Description</b>              | Configurations of SignatureVerify primitives |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmSignatureVerifyConfig   | 1                   | Container for configuration of a CSM signature verification interface. The container name serves as a symbolic name for the identifier of signature verification interface. |

## 10.2.29 CsmSignatureVerifyConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00094 :</b>   |
| <b>Container Name</b>           | CsmSignatureVerifyConfig  |
| <b>Parent Container</b>         | CsmSignatureVerify  |
| <b>Description</b>              | Container for configuration of a CSM signature verification interface. The container name serves as a symbolic name for the identifier of signature verification interface. |
| <b>Configuration Parameters</b> |   |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00096 :</b>   |    |              |
| <b>Name</b>                             | CsmSignatureVerifyAlgorithmFamily   |    |              |
| <b>Parent Container</b>                 | CsmSignatureVerifyConfig  |    |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |    |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_BRAINPOOL  |    | 0x15         |
|   | CRYPTO_ALGOFAM_CUSTOM   |    | 0xFF         |
|   | CRYPTO_ALGOFAM_ECCNIST  |    | 0x16         |
|   | CRYPTO_ALGOFAM_ED25519  |    | 0x14         |
|   | CRYPTO_ALGOFAM_RSA  |    | 0x13         |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                         |   |
|-------------------------|---|
| <b>SWS Item</b>         | <b>ECUC_Csm_00171 :</b>   |
| <b>Name</b>             | CsmSignatureVerifyAlgorithmFamilyCustom   |
| <b>Parent Container</b> | CsmSignatureVerifyConfig  |
| <b>Description</b>      | Name of the custom algorithm family used for the crypto service. This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as |

|   |                                    |    |              |
|---|------------------------------------|----|--------------|
|   | CsmSignatureVerifyAlgorithmFamily. |    |              |
| <b>Multiplicity</b>                     | 0..1                               |    |              |
| <b>Type</b>                             | EcucStringParamDef                 |    |              |
| <b>Default value</b>                    | --                                 |    |              |
| <b>maxLength</b>                        | --                                 |    |              |
| <b>minLength</b>                        | --                                 |    |              |
| <b>regularExpression</b>                | --                                 |    |              |
| <b>Post-Build Variant Value</b>         | false                              |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>            | X  | All Variants |
|   | <b>Link time</b>                   | -- |              |
|   | <b>Post-build time</b>             | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>            | X  | All Variants |
|   | <b>Link time</b>                   | -- |              |
|   | <b>Post-build time</b>             | -- |              |
| <b>Scope / Dependency</b>               | scope: local                       |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00098 :</b>                                   |    |              |
| <b>Name</b>                             | CsmSignatureVerifyAlgorithmMode                           |    |              |
| <b>Parent Container</b>                 | CsmSignatureVerifyConfig                                  |    |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |    |              |
| <b>Range</b>                            | CRYPTO_ALGOMODE_CUSTOM                                    |    | 0xFF         |
|   | CRYPTO_ALGOMODE_NOT_SET                                   |    | 0x00         |
|   | CRYPTO_ALGOMODE_RSASSA_PKCS1_v1_5                         |    | 0x0B         |
|   | CRYPTO_ALGOMODE_RSASSA_PSS                                |    | 0x0A         |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                    | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00174 :</b>                                       |    |              |
| <b>Name</b>                             | CsmSignatureVerifyAlgorithmModeCustom                         |    |              |
| <b>Parent Container</b>                 | CsmSignatureVerifyConfig                                      |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                       | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00172 :</b>   |      |              |
| <b>Name</b>                             | CsmSignatureVerifyAlgorithmSecondaryFamily  |      |              |
| <b>Parent Container</b>                 | CsmSignatureVerifyConfig  |      |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_BLAKE_1_256  |      | 0x0F         |
|   | CRYPTO_ALGOFAM_BLAKE_1_512  |      | 0x10         |
|   | CRYPTO_ALGOFAM_BLAKE_2s_256   |      | 0x11         |
|   | CRYPTO_ALGOFAM_BLAKE_2s_512   |      | 0x12         |
|   | CRYPTO_ALGOFAM_CUSTOM   |      | 0xFF         |
|   | CRYPTO_ALGOFAM_NOT_SET  |      | 0x00         |
|   | CRYPTO_ALGOFAM_RIPEMD160  |      | 0x0E         |
|   | CRYPTO_ALGOFAM_SHA1   |      | 0x01         |
|   | CRYPTO_ALGOFAM_SHA2_224   |      | 0x02         |
|   | CRYPTO_ALGOFAM_SHA2_256   |      | 0x03         |
|   | CRYPTO_ALGOFAM_SHA2_384   |      | 0x04         |
|   | CRYPTO_ALGOFAM_SHA2_512   |      | 0x05         |
|   | CRYPTO_ALGOFAM_SHA2_512_224   |      | 0x06         |
|   | CRYPTO_ALGOFAM_SHA2_512_256   |      | 0x07         |
|   | CRYPTO_ALGOFAM_SHA3_224   |      | 0x08         |
|   | CRYPTO_ALGOFAM_SHA3_256   |      | 0x09         |
|   | CRYPTO_ALGOFAM_SHA3_384   |      | 0x0A         |
|   | CRYPTO_ALGOFAM_SHA3_512   |      | 0x0B         |
| CRYPTO_ALGOFAM_SHAKE128                 |   | 0x0C |              |
| CRYPTO_ALGOFAM_SHAKE256                 |   | 0x0D |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>               | scope: local  |      |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00173 :</b>  |    |              |
| <b>Name</b>                             | CsmSignatureVerifyAlgorithmSecondaryFamilyCustom   |    |              |
| <b>Parent Container</b>                 | CsmSignatureVerifyConfig   |    |              |
| <b>Description</b>                      | Name of the custom secondary algorithm family used for the crypto service. This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmSignatureVerifyAlgorithmFamily. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucStringParamDef   |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |

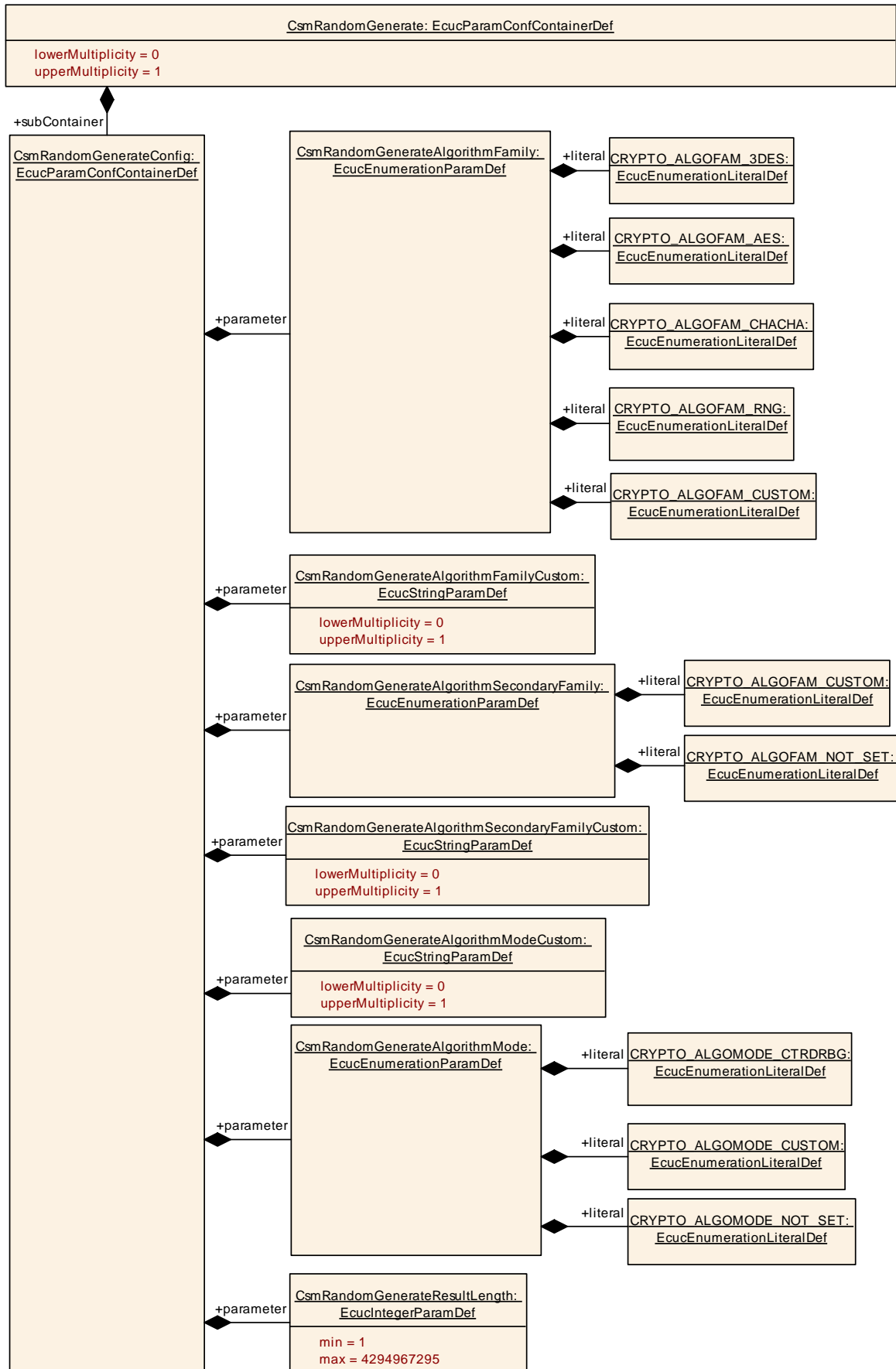
|                           |                        |    |  |
|---------------------------|------------------------|----|--|
|                           | <b>Link time</b>       | -- |  |
|                           | <b>Post-build time</b> | -- |  |
| <b>Scope / Dependency</b> | scope: local           |    |  |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00176 :</b>   |    |              |
| <b>Name</b>                             | CsmSignatureVerifyCompareLength   |    |              |
| <b>Parent Container</b>                 | CsmSignatureVerifyConfig  |    |              |
| <b>Description</b>                      | Number of the least significant bytes of the signature, for which the verification shall be calculated. |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef   |    |              |
| <b>Range</b>                            | 1 .. 4294967295   |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00175 :</b>  |    |              |
| <b>Name</b>                             | CsmSignatureVerifyDataMaxLength  |    |              |
| <b>Parent Container</b>                 | CsmSignatureVerifyConfig   |    |              |
| <b>Description</b>                      | Max size of the input data, for which the signature shall be verified, in bytes. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef  |    |              |
| <b>Range</b>                            | 1 .. 4294967295  |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00192 :</b>                   |    |              |
| <b>Name</b>                             | CsmSignatureVerifyKeyLength               |    |              |
| <b>Parent Container</b>                 | CsmSignatureVerifyConfig                  |    |              |
| <b>Description</b>                      | Size of the signature verify key in bytes |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                       |    |              |
| <b>Range</b>                            | 1 .. 4294967295                           |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>Post-Build Variant Value</b>         | false                                     |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                   | X  | All Variants |
|   | <b>Link time</b>                          | -- |              |
|   | <b>Post-build time</b>                    | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                   | X  | All Variants |
|   | <b>Link time</b>                          | -- |              |
|   | <b>Post-build time</b>                    | -- |              |
| <b>Scope / Dependency</b>               | scope: local                              |    |              |

***No Included Containers***



**Figure 9-18 CsmRandomGenerate Layout**

### 10.2.30 CsmRandomGenerate

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00031 :</b>                     |
| <b>Container Name</b>           | CsmRandomGenerate                           |
| <b>Parent Container</b>         | CsmPrimitives                               |
| <b>Description</b>              | Configurations of RandomGenerate primitives |
| <b>Configuration Parameters</b> |   |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmRandomGenerateConfig    | 1                   | Container for configuration of a CSM random generator. The container name serves as a symbolic name for the identifier of a random generator configuration. |

### 10.2.31 CsmRandomGenerateConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00103 :</b>   |
| <b>Container Name</b>           | CsmRandomGenerateConfig   |
| <b>Parent Container</b>         | CsmRandomGenerate   |
| <b>Description</b>              | Container for configuration of a CSM random generator. The container name serves as a symbolic name for the identifier of a random generator configuration. |
| <b>Configuration Parameters</b> |   |

|                         |   |      |
|-------------------------|---|------|
| <b>SWS Item</b>         | <b>ECUC_Csm_00105 :</b>   |      |
| <b>Name</b>             | CsmRandomGenerateAlgorithmFamily  |      |
| <b>Parent Container</b> | CsmRandomGenerateConfig   |      |
| <b>Description</b>      | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |
| <b>Multiplicity</b>     | 1   |      |
| <b>Type</b>             | EcucEnumerationParamDef   |      |
| <b>Range</b>            | CRYPTO_ALGOFAM_3DES   | 0x13 |
|                         | CRYPTO_ALGOFAM_AES  | 0x14 |
|                         | CRYPTO_ALGOFAM_BLAKE_1_256  | 0x0F |
|                         | CRYPTO_ALGOFAM_BLAKE_1_512  | 0x10 |
|                         | CRYPTO_ALGOFAM_BLAKE_2s_256   | 0x11 |
|                         | CRYPTO_ALGOFAM_BLAKE_2s_512   | 0x12 |
|                         | CRYPTO_ALGOFAM_CHACHA   | 0x15 |
|                         | CRYPTO_ALGOFAM_CUSTOM   | 0xFF |
|                         | CRYPTO_ALGOFAM_RIPEMD160  | 0x0E |
|                         | CRYPTO_ALGOFAM_RNG  | 0x1B |
|                         | CRYPTO_ALGOFAM_SHA1   | 0x01 |
|                         | CRYPTO_ALGOFAM_SHA2_224   | 0x02 |
|                         | CRYPTO_ALGOFAM_SHA2_256   | 0x03 |
|                         | CRYPTO_ALGOFAM_SHA2_384   | 0x04 |
|                         | CRYPTO_ALGOFAM_SHA2_512   | 0x05 |
|                         | CRYPTO_ALGOFAM_SHA2_512_224   | 0x06 |
|                         | CRYPTO_ALGOFAM_SHA2_512_256   | 0x07 |
|                         | CRYPTO_ALGOFAM_SHA3_224   | 0x08 |
|                         | CRYPTO_ALGOFAM_SHA3_256   | 0x09 |
|                         | CRYPTO_ALGOFAM_SHA3_384   | 0x0A |
|                         | CRYPTO_ALGOFAM_SHA3_512   | 0x0B |
|                         | CRYPTO_ALGOFAM_SHAKE128   | 0x0C |

|   |                         |                |
|---|-------------------------|----------------|
|   | CRYPTO_ALGOFAM_SHAKE256 | 0x0D           |
| <b>Post-Build Variant Value</b>         | false                   |                |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X All Variants |
|   | <b>Link time</b>        | --             |
|   | <b>Post-build time</b>  | --             |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X All Variants |
|   | <b>Link time</b>        | --             |
|   | <b>Post-build time</b>  | --             |
| <b>Scope / Dependency</b>               | scope: local            |                |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00177 :</b>  |    |              |
| <b>Name</b>                             | CsmRandomGenerateAlgorithmFamilyCustom   |    |              |
| <b>Parent Container</b>                 | CsmRandomGenerateConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm family used for the crypto service. This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmRandomAlgorithmFamily |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucStringParamDef   |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|   |   |      |              |
|---|---|------|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00107 :</b>                                   |      |              |
| <b>Name</b>                             | CsmRandomGenerateAlgorithmMode                            |      |              |
| <b>Parent Container</b>                 | CsmRandomGenerateConfig                                   |      |              |
| <b>Description</b>                      | Determines the algorithm mode used for the crypto service |      |              |
| <b>Multiplicity</b>                     | 1   |      |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                   |      |              |
| <b>Range</b>                            | CRYPTO_ALGOMODE_CMAC                                      | 0x10 |              |
|   | CRYPTO_ALGOMODE_CTRDRBG                                   | 0x12 |              |
|   | CRYPTO_ALGOMODE_CUSTOM                                    | 0xFF |              |
|   | CRYPTO_ALGOMODE_GMAC                                      | 0x11 |              |
|   | CRYPTO_ALGOMODE_HMAC                                      | 0x0f |              |
|   | CRYPTO_ALGOMODE_NOT_SET                                   | 0x00 |              |
|   | CRYPTO_ALGOMODE_SIPHASH_2_4                               | 0x17 |              |
|   | CRYPTO_ALGOMODE_SIPHASH_4_8                               | 0x18 |              |
| <b>Post-Build Variant Value</b>         | false   |      |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>                                    | --   |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                   | X    | All Variants |
|   | <b>Link time</b>  | --   |              |
|   | <b>Post-build time</b>                                    | --   |              |
| <b>Scope /</b>                          | scope: local  |      |              |



| Dependency                              |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00180 :</b>   |    |              |
| <b>Name</b>                             | CsmRandomGenerateAlgorithmModeCustom  |    |              |
| <b>Parent Container</b>                 | CsmRandomGenerateConfig   |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service. This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used as CsmRandomGenerateAlgorithmFamily. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00178 :</b>                                     |    |              |
| <b>Name</b>                             | CsmRandomGenerateAlgorithmSecondaryFamily                   |    |              |
| <b>Parent Container</b>                 | CsmRandomGenerateConfig                                     |    |              |
| <b>Description</b>                      | Determines the algorithm family used for the crypto service |    |              |
| <b>Multiplicity</b>                     | 1   |    |              |
| <b>Type</b>                             | EcucEnumerationParamDef                                     |    |              |
| <b>Range</b>                            | CRYPTO_ALGOFAM_CUSTOM                                       |    | 0xFF         |
|   | CRYPTO_ALGOFAM_NOT_SET                                      |    | 0x00         |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                                     | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                      | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                                     | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>                                      | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                          |  |  |  |
|--------------------------|--|--|--|
| <b>SWS Item</b>          | <b>ECUC_Csm_00179 :</b>  |  |  |
| <b>Name</b>              | CsmRandomGenerateAlgorithmSecondaryFamilyCustom  |  |  |
| <b>Parent Container</b>  | CsmRandomGenerateConfig  |  |  |
| <b>Description</b>       | Name of the custom secondary algorithm family used for the crypto service. This is the second name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is set as CsmRandomAlgorithmSecondaryFamily. |  |  |
| <b>Multiplicity</b>      | 0..1   |  |  |
| <b>Type</b>              | EcucStringParamDef   |  |  |
| <b>Default value</b>     | --   |  |  |
| <b>maxLength</b>         | --   |  |  |
| <b>minLength</b>         | --   |  |  |
| <b>regularExpression</b> | --   |  |  |

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

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00106 :</b>                  |    |              |
| <b>Name</b>                             | CsmRandomGenerateResultLength            |    |              |
| <b>Parent Container</b>                 | CsmRandomGenerateConfig                  |    |              |
| <b>Description</b>                      | Size of the random generate key in bytes |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | EcucIntegerParamDef                      |    |              |
| <b>Range</b>                            | 1 .. 4294967295                          |    |              |
| <b>Default value</b>                    | --                                       |    |              |
| <b>Post-Build Variant Value</b>         | false                                    |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                  | X  | All Variants |
|   | <b>Link time</b>                         | -- |              |
|   | <b>Post-build time</b>                   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                  | X  | All Variants |
|   | <b>Link time</b>                         | -- |              |
|   | <b>Post-build time</b>                   | -- |              |
| <b>Scope / Dependency</b>               | scope: local                             |    |              |

**No Included Containers**

### 10.2.32 CsmJobKeySetValid

|                                 |  |  |  |
|---------------------------------|--|--|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00196 :</b>                  |  |  |
| <b>Container Name</b>           | CsmJobKeySetValid                        |  |  |
| <b>Parent Container</b>         | CsmPrimitives                            |  |  |
| <b>Description</b>              | Configurations of KeySetValid primitives |  |  |
| <b>Configuration Parameters</b> |  |  |  |

|                            |                     |   |  |
|----------------------------|---------------------|---|--|
| <b>Included Containers</b> |                     |   |  |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |  |
| CsmJobKeySetValidConfig    | 1                   | Container for configuration of a CSM key set valid operation. The container name serves as a symbolic name for the identifier of a key configuration. |  |

### 10.2.33 CsmJobKeySetValidConfig

|                                 |   |  |  |
|---------------------------------|---|--|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00204 :</b>   |  |  |
| <b>Container Name</b>           | CsmJobKeySetValidConfig   |  |  |
| <b>Parent Container</b>         | CsmJobKeySetValid   |  |  |
| <b>Description</b>              | Container for configuration of a CSM key set valid operation. The container name serves as a symbolic name for the identifier of a key configuration. |  |  |
| <b>Configuration Parameters</b> |   |  |  |

***No Included Containers***

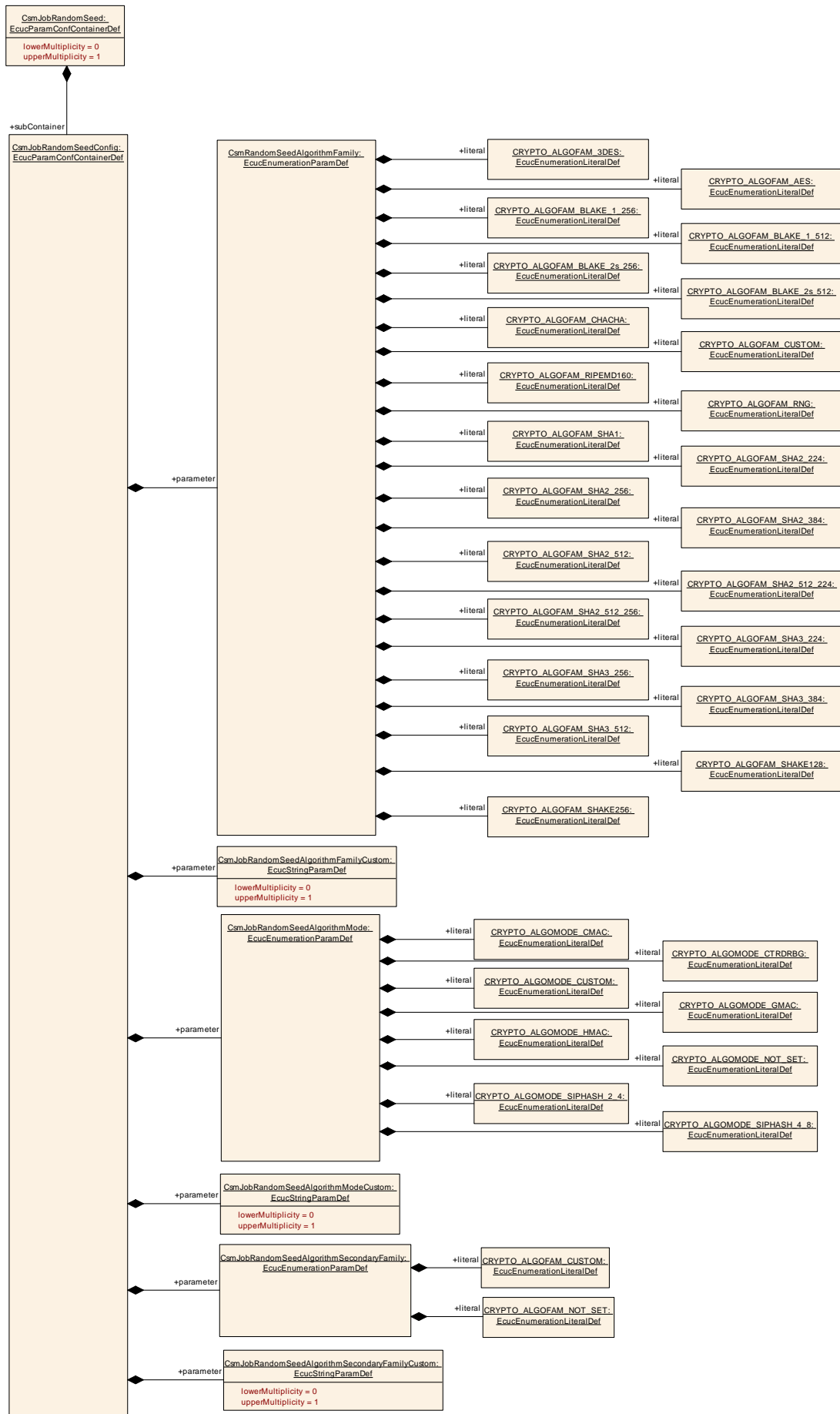


Figure 9-19 CsmJobRandomSeed Layout

## 10.2.34 CsmJobRandomSeed

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00197 :</b>                 |
| <b>Container Name</b>           | CsmJobRandomSeed                        |
| <b>Parent Container</b>         | CsmPrimitives                           |
| <b>Description</b>              | Configurations of RandomSeed primitives |
| <b>Configuration Parameters</b> |   |

|                            |                     |   |
|----------------------------|---------------------|---|
| <b>Included Containers</b> |                     |   |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmJobRandomSeedConfig     | 1                   | Container for configuration of a CSM Random Seed operation. The container name serves as a symbolic name for the identifier of a random seed configuration. |

## 10.2.35 CsmJobRandomSeedConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00261 :</b>   |
| <b>Container Name</b>           | CsmJobRandomSeedConfig  |
| <b>Parent Container</b>         | CsmJobRandomSeed  |
| <b>Description</b>              | Container for configuration of a CSM random seed operation. The container name serves as a symbolic name for the identifier of a random seed configuration. |
| <b>Configuration Parameters</b> |   |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00207 :</b>   |    |              |
| <b>Name</b>                             | CsmJobRandomSeedAlgorithmFamilyCustom   |    |              |
| <b>Parent Container</b>                 | CsmJobRandomSeedConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm family used for the crypto service. This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                         |                               |
|-------------------------|-------------------------------|
| <b>SWS Item</b>         | <b>ECUC_Csm_00208 :</b>       |
| <b>Name</b>             | CsmJobRandomSeedAlgorithmMode |
| <b>Parent Container</b> | CsmJobRandomSeedConfig        |

|                                  |   |      |              |
|----------------------------------|---|------|--------------|
| <b>Description</b>               | Determines the algorithm mode used for the crypto service |      |              |
| <b>Multiplicity</b>              | 1   |      |              |
| <b>Type</b>                      | EcucEnumerationParamDef                                   |      |              |
| <b>Range</b>                     | CRYPTO_ALGOMODE_CMAC                                      |      | 0x10         |
|                                  | CRYPTO_ALGOMODE_CTRDRBG                                   |      | 0x12         |
|                                  | CRYPTO_ALGOMODE_CUSTOM                                    |      | 0xFF         |
|                                  | CRYPTO_ALGOMODE_GMAC                                      |      | 0x11         |
|                                  | CRYPTO_ALGOMODE_HMAC                                      |      | 0x0f         |
|                                  | CRYPTO_ALGOMODE_NOT_SET                                   |      | 0x00         |
|                                  | CRYPTO_ALGOMODE_SIPHASH_2_4                               |      | 0x17         |
| CRYPTO_ALGOMODE_SIPHASH_4_8      |   | 0x18 |              |
| <b>Post-Build Variant Value</b>  | false   |      |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>                                   | X    | All Variants |
|                                  | <b>Link time</b>  | --   |              |
|                                  | <b>Post-build time</b>                                    | --   |              |
| <b>Scope / Dependency</b>        | scope: local  |      |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00209 :</b>   |    |              |
| <b>Name</b>                             | CsmJobRandomSeedAlgorithmModeCustom   |    |              |
| <b>Parent Container</b>                 | CsmJobRandomSeedConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service. This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                                  |  |    |              |
|----------------------------------|--|----|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00210 :</b>                                      |    |              |
| <b>Name</b>                      | CsmJobRandomSeedAlgorithmSecondaryFamily                     |    |              |
| <b>Parent Container</b>          | CsmJobRandomSeedConfig                                       |    |              |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. |    |              |
| <b>Multiplicity</b>              | 1  |    |              |
| <b>Type</b>                      | EcucEnumerationParamDef                                      |    |              |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM  |    | 0xFF         |
|                                  | CRYPTO_ALGOFAM_NOT_SET                                       |    | 0x0f         |
| <b>Post-Build Variant Value</b>  | false  |    |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>                                      | X  | All Variants |
|                                  | <b>Link time</b>   | -- |              |
|                                  | <b>Post-build time</b>                                       | -- |              |
| <b>Scope /</b>                   | scope: local   |    |              |

|                   |  |
|-------------------|--|
| <b>Dependency</b> |  |
|-------------------|--|

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00211 :</b>  |    |              |
| <b>Name</b>                             | CsmJobRandomSeedAlgorithmSecondaryFamilyCustom   |    |              |
| <b>Parent Container</b>                 | CsmJobRandomSeedConfig   |    |              |
| <b>Description</b>                      | Name of the custom secondary algorithm family used for the crypto service. This is the second name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucStringParamDef   |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|                           |   |      |      |
|---------------------------|---|------|------|
| <b>SWS Item</b>           | <b>ECUC_Csm_00206 :</b>   |      |      |
| <b>Name</b>               | CsmRandomSeedAlgorithmFamily  |      |      |
| <b>Parent Container</b>   | CsmJobRandomSeedConfig  |      |      |
| <b>Description</b>        | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |      |
| <b>Multiplicity</b>       | 1   |      |      |
| <b>Type</b>               | EcucEnumerationParamDef   |      |      |
| <b>Range</b>              | CRYPTO_ALGOFAM_3DES   |      | 0x13 |
|                           | CRYPTO_ALGOFAM_AES  |      | 0x14 |
|                           | CRYPTO_ALGOFAM_BLAKE_1_256  |      | 0x0F |
|                           | CRYPTO_ALGOFAM_BLAKE_1_512  |      | 0x10 |
|                           | CRYPTO_ALGOFAM_BLAKE_2s_256   |      | 0x11 |
|                           | CRYPTO_ALGOFAM_BLAKE_2s_512   |      | 0x12 |
|                           | CRYPTO_ALGOFAM_CHACHA   |      | 0x15 |
|                           | CRYPTO_ALGOFAM_CUSTOM   |      | 0xFF |
|                           | CRYPTO_ALGOFAM_RIPEMD160  |      | 0x0E |
|                           | CRYPTO_ALGOFAM_RNG  |      | 0x1B |
|                           | CRYPTO_ALGOFAM_SHA1   |      | 0x01 |
|                           | CRYPTO_ALGOFAM_SHA2_224   |      | 0x02 |
|                           | CRYPTO_ALGOFAM_SHA2_256   |      | 0x03 |
|                           | CRYPTO_ALGOFAM_SHA2_384   |      | 0x04 |
|                           | CRYPTO_ALGOFAM_SHA2_512   |      | 0x05 |
|                           | CRYPTO_ALGOFAM_SHA2_512_224   |      | 0x06 |
|                           | CRYPTO_ALGOFAM_SHA2_512_256   |      | 0x07 |
|                           | CRYPTO_ALGOFAM_SHA3_224   |      | 0x08 |
|                           | CRYPTO_ALGOFAM_SHA3_256   |      | 0x09 |
|                           | CRYPTO_ALGOFAM_SHA3_384   |      | 0x0A |
| CRYPTO_ALGOFAM_SHA3_512   |   | 0x0B |      |
| CRYPTO_ALGOFAM_SHAKE128   |   | 0x0C |      |
| CRYPTO_ALGOFAM_SHAKE256   |   | 0x0D |      |
| <b>Post-Build Variant</b> | false   |      |      |

|                            |                         |    |              |
|----------------------------|-------------------------|----|--------------|
| <b>Value</b>               |                         |    |              |
| <b>Value</b>               | <b>Pre-compile time</b> | X  | All Variants |
| <b>Configuration Class</b> | <b>Link time</b>        | -- |              |
| <b>Scope / Dependency</b>  | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>  | scope: local            |    |              |

**No Included Containers**

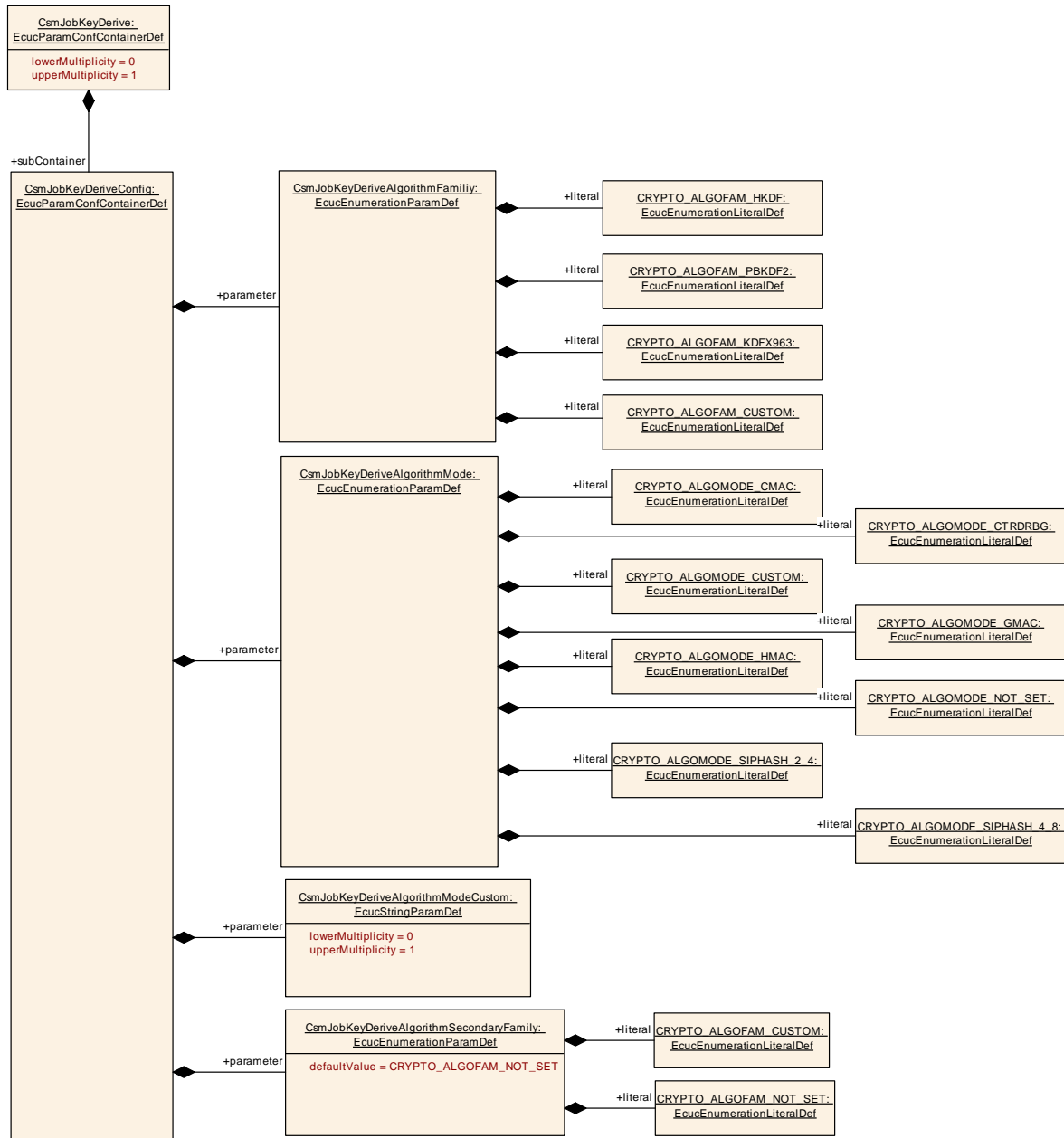


Figure 9-20 CsmJobKeyDerive Layout

10.2.36 CsmJobKeyDerive

|                 |                         |
|-----------------|-------------------------|
| <b>SWS Item</b> | <b>ECUC_Csm_00198 :</b> |
|-----------------|-------------------------|



|                                 |  |
|---------------------------------|--|
| <b>Container Name</b>           | CsmJobKeyDerive                        |
| <b>Parent Container</b>         | CsmPrimitives                          |
| <b>Description</b>              | Configurations of KeyDerive primitives |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmJobKeyDeriveConfig      | 1                   | Container for configuration of a CSM key derive operation. The container name serves as a symbolic name for the identifier of a key derive configuration. |

### 10.2.37 CsmJobKeyDeriveConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00213 :</b>   |
| <b>Container Name</b>           | CsmJobKeyDeriveConfig   |
| <b>Parent Container</b>         | CsmJobKeyDerive   |
| <b>Description</b>              | Container for configuration of a CSM key derive operation. The container name serves as a symbolic name for the identifier of a key derive configuration. |
| <b>Configuration Parameters</b> |   |

|                                  |   |    |              |
|----------------------------------|---|----|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00215 :</b>   |    |              |
| <b>Name</b>                      | CsmJobKeyDeriveAlgorithmFamily  |    |              |
| <b>Parent Container</b>          | CsmJobKeyDeriveConfig   |    |              |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |    |              |
| <b>Multiplicity</b>              | 1   |    |              |
| <b>Type</b>                      | EcucEnumerationParamDef   |    |              |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM   |    | 0xFF         |
|                                  | CRYPTO_ALGOFAM_HKDF   |    | --           |
|                                  | CRYPTO_ALGOFAM_KDFX963  |    | 0x25         |
|                                  | CRYPTO_ALGOFAM_PBKDF2   |    | 0x24         |
| <b>Post-Build Variant Value</b>  | false   |    |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|                                  | <b>Link time</b>  | -- |              |
|                                  | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>        | scope: local  |    |              |

|                         |   |  |      |
|-------------------------|---|--|------|
| <b>SWS Item</b>         | <b>ECUC_Csm_00216 :</b>                                   |  |      |
| <b>Name</b>             | CsmJobKeyDeriveAlgorithmMode                              |  |      |
| <b>Parent Container</b> | CsmJobKeyDeriveConfig                                     |  |      |
| <b>Description</b>      | Determines the algorithm mode used for the crypto service |  |      |
| <b>Multiplicity</b>     | 1   |  |      |
| <b>Type</b>             | EcucEnumerationParamDef                                   |  |      |
| <b>Range</b>            | CRYPTO_ALGOMODE_CMAC                                      |  | 0x10 |
|                         | CRYPTO_ALGOMODE_CTRDRBG                                   |  | 0x12 |
|                         | CRYPTO_ALGOMODE_CUSTOM                                    |  | 0xFF |
|                         | CRYPTO_ALGOMODE_GMAC                                      |  | 0x11 |
|                         | CRYPTO_ALGOMODE_HMAC                                      |  | 0x0f |
|                         | CRYPTO_ALGOMODE_NOT_SET                                   |  | 0x00 |
|                         | CRYPTO_ALGOMODE_SIPHASH_2_4                               |  | 0x17 |

|                                  |                             |                |
|----------------------------------|-----------------------------|----------------|
|                                  | CRYPTO_ALGOMODE_SIPHASH_4_8 | 0x18           |
| <b>Post-Build Variant Value</b>  | false                       |                |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>     | X All Variants |
|                                  | <b>Link time</b>            | --             |
|                                  | <b>Post-build time</b>      | --             |
| <b>Scope / Dependency</b>        | scope: local                |                |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00217 :</b>  |    |              |
| <b>Name</b>                             | CsmJobKeyDeriveAlgorithmModeCustom                             |    |              |
| <b>Parent Container</b>                 | CsmJobKeyDeriveConfig  |    |              |
| <b>Description</b>                      | Name of the custom algorithm mode used for the crypto service. |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucStringParamDef   |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

|                                  |  |      |              |
|----------------------------------|--|------|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00218 :</b>                                      |      |              |
| <b>Name</b>                      | CsmJobKeyDeriveAlgorithmSecondaryFamily                      |      |              |
| <b>Parent Container</b>          | CsmJobKeyDeriveConfig  |      |              |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. |      |              |
| <b>Multiplicity</b>              | 1  |      |              |
| <b>Type</b>                      | EcucEnumerationParamDef                                      |      |              |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM  | 0xFF |              |
|                                  | CRYPTO_ALGOFAM_NOT_SET                                       | 0x00 |              |
| <b>Default value</b>             | CRYPTO_ALGOFAM_NOT_SET                                       |      |              |
| <b>Post-Build Variant Value</b>  | false  |      |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>                                      | X    | All Variants |
|                                  | <b>Link time</b>   | --   |              |
|                                  | <b>Post-build time</b>                                       | --   |              |
| <b>Scope / Dependency</b>        | scope: local   |      |              |

**No Included Containers**

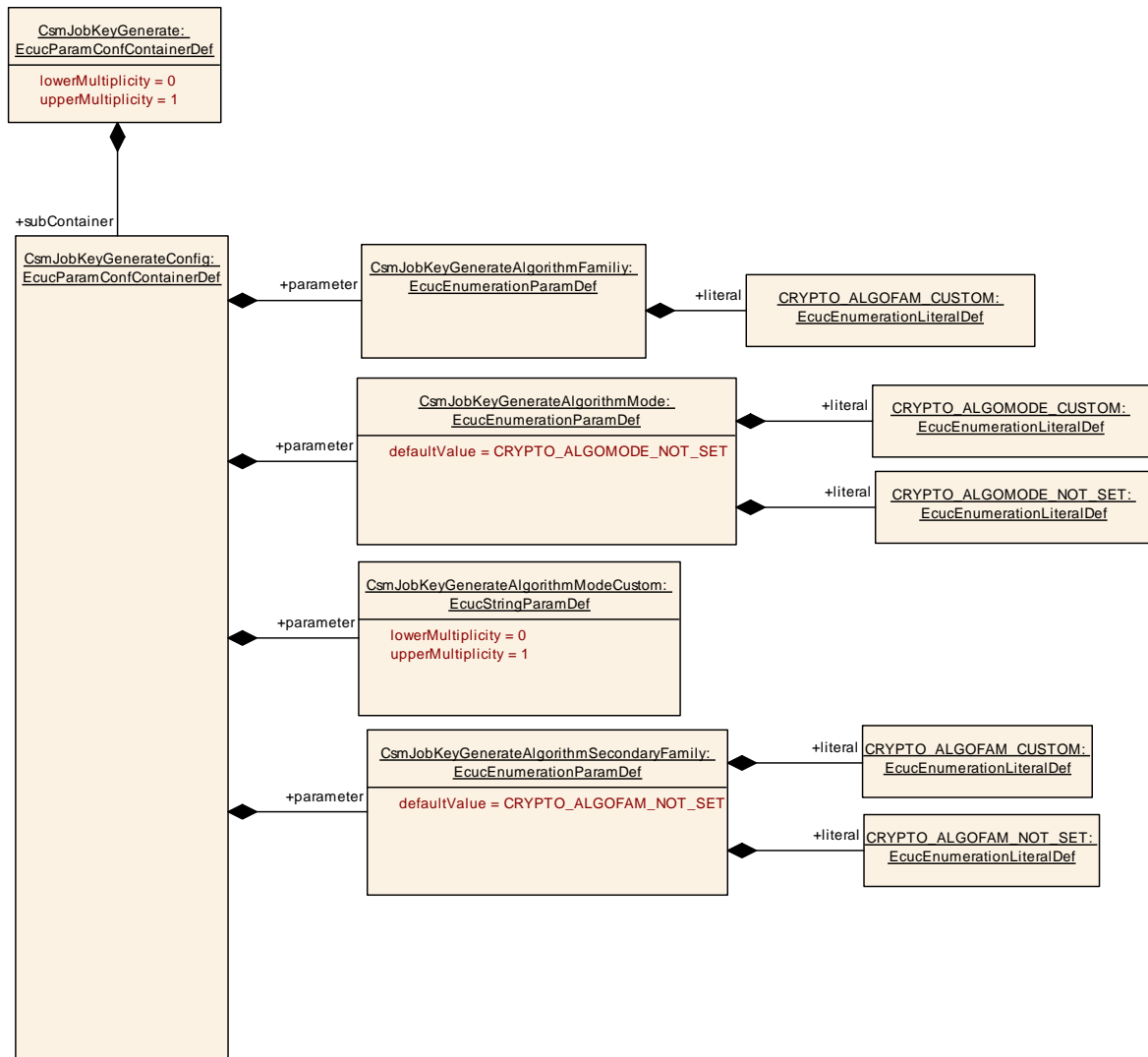


Figure 9-21 CsmJobKeyGenerate Layout

### 10.2.38 CsmJobKeyGenerate

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | ECUC_Csm_00199 :                         |
| <b>Container Name</b>           | CsmJobKeyGenerate                        |
| <b>Parent Container</b>         | CsmPrimitives                            |
| <b>Description</b>              | Configurations of KeyGenerate primitives |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmJobKeyGenerateConfig    | 1                   | Container for configuration of a CSM key generate operation. The container name serves as a symbolic name for the identifier of a key generate configuration. |

## 10.2.39 CsmJobKeyGenerateConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00220 :</b>   |
| <b>Container Name</b>           | CsmJobKeyGenerateConfig   |
| <b>Parent Container</b>         | CsmJobKeyGenerate   |
| <b>Description</b>              | Container for configuration of a CSM key generate operation. The container name serves as a symbolic name for the identifier of a key generate configuration. |
| <b>Configuration Parameters</b> |   |

|                                  |  |                         |   |              |                  |    |  |                        |    |  |
|----------------------------------|--|-------------------------|---|--------------|------------------|----|--|------------------------|----|--|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00222 :</b>  |                         |   |              |                  |    |  |                        |    |  |
| <b>Name</b>                      | CsmJobKeyGenerateAlgorithmFamily   |                         |   |              |                  |    |  |                        |    |  |
| <b>Parent Container</b>          | CsmJobKeyGenerateConfig  |                         |   |              |                  |    |  |                        |    |  |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm.  |                         |   |              |                  |    |  |                        |    |  |
| <b>Multiplicity</b>              | 1  |                         |   |              |                  |    |  |                        |    |  |
| <b>Type</b>                      | EcucEnumerationParamDef  |                         |   |              |                  |    |  |                        |    |  |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM   0xFF   |                         |   |              |                  |    |  |                        |    |  |
| <b>Post-Build Variant Value</b>  | false  |                         |   |              |                  |    |  |                        |    |  |
| <b>Value Configuration Class</b> | <table border="1"> <tr> <td><b>Pre-compile time</b></td> <td>X</td> <td>All Variants</td> </tr> <tr> <td><b>Link time</b></td> <td>--</td> <td></td> </tr> <tr> <td><b>Post-build time</b></td> <td>--</td> <td></td> </tr> </table> | <b>Pre-compile time</b> | X | All Variants | <b>Link time</b> | -- |  | <b>Post-build time</b> | -- |  |
| <b>Pre-compile time</b>          | X  | All Variants            |   |              |                  |    |  |                        |    |  |
| <b>Link time</b>                 | --   |                         |   |              |                  |    |  |                        |    |  |
| <b>Post-build time</b>           | --   |                         |   |              |                  |    |  |                        |    |  |
| <b>Scope / Dependency</b>        | scope: local   |                         |   |              |                  |    |  |                        |    |  |

|                                  |  |                         |   |              |                  |    |  |                        |    |  |
|----------------------------------|--|-------------------------|---|--------------|------------------|----|--|------------------------|----|--|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00223 :</b>  |                         |   |              |                  |    |  |                        |    |  |
| <b>Name</b>                      | CsmJobKeyGenerateAlgorithmMode   |                         |   |              |                  |    |  |                        |    |  |
| <b>Parent Container</b>          | CsmJobKeyGenerateConfig  |                         |   |              |                  |    |  |                        |    |  |
| <b>Description</b>               | Determines the algorithm mode used for the crypto service  |                         |   |              |                  |    |  |                        |    |  |
| <b>Multiplicity</b>              | 1  |                         |   |              |                  |    |  |                        |    |  |
| <b>Type</b>                      | EcucEnumerationParamDef  |                         |   |              |                  |    |  |                        |    |  |
| <b>Range</b>                     | CRYPTO_ALGOMODE_CUSTOM   0xFF<br>CRYPTO_ALGOMODE_NOT_SET   0x00  |                         |   |              |                  |    |  |                        |    |  |
| <b>Default value</b>             | CRYPTO_ALGOMODE_NOT_SET  |                         |   |              |                  |    |  |                        |    |  |
| <b>Post-Build Variant Value</b>  | false  |                         |   |              |                  |    |  |                        |    |  |
| <b>Value Configuration Class</b> | <table border="1"> <tr> <td><b>Pre-compile time</b></td> <td>X</td> <td>All Variants</td> </tr> <tr> <td><b>Link time</b></td> <td>--</td> <td></td> </tr> <tr> <td><b>Post-build time</b></td> <td>--</td> <td></td> </tr> </table> | <b>Pre-compile time</b> | X | All Variants | <b>Link time</b> | -- |  | <b>Post-build time</b> | -- |  |
| <b>Pre-compile time</b>          | X  | All Variants            |   |              |                  |    |  |                        |    |  |
| <b>Link time</b>                 | --   |                         |   |              |                  |    |  |                        |    |  |
| <b>Post-build time</b>           | --   |                         |   |              |                  |    |  |                        |    |  |
| <b>Scope / Dependency</b>        | scope: local   |                         |   |              |                  |    |  |                        |    |  |

|  |  |
|--|--|
| <b>SWS Item</b>                        | <b>ECUC_Csm_00224 :</b>  |
| <b>Name</b>                            | CsmJobKeyGenerateAlgorithmModeCustom                           |
| <b>Parent Container</b>                | CsmJobKeyGenerateConfig  |
| <b>Description</b>                     | Name of the custom algorithm mode used for the crypto service. |
| <b>Multiplicity</b>                    | 0..1   |
| <b>Type</b>                            | EcucStringParamDef   |
| <b>Default value</b>                   | --   |
| <b>maxLength</b>                       | --   |
| <b>minLength</b>                       | --   |
| <b>regularExpression</b>               | --   |
| <b>Post-Build Variant Multiplicity</b> | false  |
| <b>Post-Build Variant Value</b>        | false  |

|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

|                                  |  |    |              |
|----------------------------------|--|----|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00225 :</b>                                      |    |              |
| <b>Name</b>                      | CsmJobKeyGenerateAlgorithmSecondaryFamily                    |    |              |
| <b>Parent Container</b>          | CsmJobKeyGenerateConfig                                      |    |              |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. |    |              |
| <b>Multiplicity</b>              | 1  |    |              |
| <b>Type</b>                      | EcucEnumerationParamDef                                      |    |              |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM  |    | 0xFF         |
|                                  | CRYPTO_ALGOFAM_NOT_SET                                       |    | 0x00         |
| <b>Default value</b>             | CRYPTO_ALGOFAM_NOT_SET                                       |    |              |
| <b>Post-Build Variant Value</b>  | false  |    |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>                                      | X  | All Variants |
|                                  | <b>Link time</b>   | -- |              |
|                                  | <b>Post-build time</b>                                       | -- |              |
| <b>Scope / Dependency</b>        | scope: local   |    |              |

**No Included Containers**

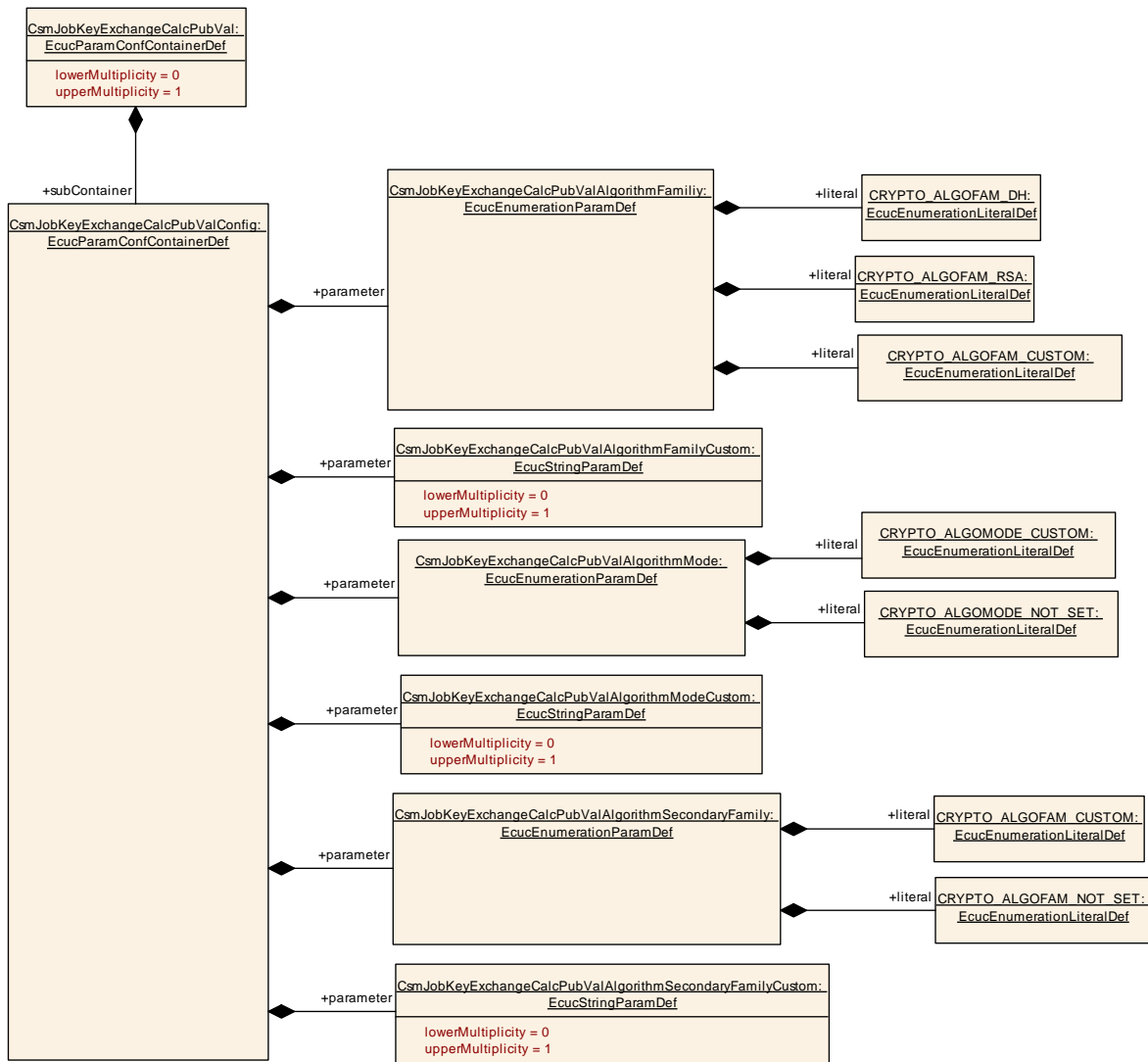


Figure 9-22 CsmJobKeyExchangeCalcPubVal Layout

10.2.40 CsmJobKeyExchangeCalcPubVal

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00200 :</b>                            |
| <b>Container Name</b>           | CsmJobKeyExchangeCalcPubVal                        |
| <b>Parent Container</b>         | CsmPrimitives                                      |
| <b>Description</b>              | Configurations of KeyExchangeCalcPubVal primitives |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b>        |                     |  |
|-----------------------------------|---------------------|--|
| <b>Container Name</b>             | <b>Multiplicity</b> | <b>Scope / Dependency</b>  |
| CsmJobKeyExchangeCalcPubValConfig | 1                   | Container for configuration of a CSM JobKeyExchangeCalcPubVal. The container name serves as a symbolic name for the identifier of a key configuration. |

## 10.2.41 CsmJobKeyExchangeCalcPubValConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00226 :</b>  |
| <b>Container Name</b>           | CsmJobKeyExchangeCalcPubValConfig  |
| <b>Parent Container</b>         | CsmJobKeyExchangeCalcPubVal  |
| <b>Description</b>              | Container for configuration of a CSM JobKeyExchangeCalcPubVal. The container name serves as a symbolic name for the identifier of a key configuration. |
| <b>Configuration Parameters</b> |  |

|                                  |   |      |              |
|----------------------------------|---|------|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00227 :</b>   |      |              |
| <b>Name</b>                      | CsmJobKeyExchangeCalcPubValAlgorithmFamily  |      |              |
| <b>Parent Container</b>          | CsmJobKeyExchangeCalcPubValConfig   |      |              |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |              |
| <b>Multiplicity</b>              | 1   |      |              |
| <b>Type</b>                      | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM   | 0xFF |              |
|                                  | CRYPTO_ALGOFAM_DH   | 0x26 |              |
|                                  | CRYPTO_ALGOFAM_RSA  | 0x13 |              |
| <b>Post-Build Variant Value</b>  | false   |      |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|                                  | <b>Link time</b>  | --   |              |
|                                  | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>        | scope: local  |      |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00228 :</b>   |    |              |
| <b>Name</b>                             | CsmJobKeyExchangeCalcPubValAlgorithmFamilyCustom  |    |              |
| <b>Parent Container</b>                 | CsmJobKeyExchangeCalcPubValConfig   |    |              |
| <b>Description</b>                      | Name of the custom algorithm family used for the crypto service. This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                         |   |  |  |
|-------------------------|---|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00229 :</b>                                   |  |  |
| <b>Name</b>             | CsmJobKeyExchangeCalcPubValAlgorithmMode                  |  |  |
| <b>Parent Container</b> | CsmJobKeyExchangeCalcPubValConfig                         |  |  |
| <b>Description</b>      | Determines the algorithm mode used for the crypto service |  |  |
| <b>Multiplicity</b>     | 1   |  |  |

|                                  |                         |    |              |
|----------------------------------|-------------------------|----|--------------|
| <b>Type</b>                      | EcucEnumerationParamDef |    |              |
| <b>Range</b>                     | CRYPTO_ALGOMODE_CUSTOM  |    | 0xFF         |
|                                  | CRYPTO_ALGOMODE_NOT_SET |    | 0x00         |
| <b>Post-Build Variant Value</b>  | false                   |    |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|                                  | <b>Link time</b>        | -- |              |
|                                  | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>        | scope: local            |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00260 :</b>                        |    |              |
| <b>Name</b>                             | CsmJobKeyExchangeCalcPubValAlgorithmModeCustom |    |              |
| <b>Parent Container</b>                 | CsmJobKeyExchangeCalcPubValConfig              |    |              |
| <b>Description</b>                      | Name of the custom primitive mode.             |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucStringParamDef                             |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                        | X  | All Variants |
|   | <b>Link time</b>                               | -- |              |
|   | <b>Post-build time</b>                         | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                        | X  | All Variants |
|   | <b>Link time</b>                               | -- |              |
|   | <b>Post-build time</b>                         | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                   |    |              |

|                                  |  |    |              |
|----------------------------------|--|----|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00231 :</b>                                      |    |              |
| <b>Name</b>                      | CsmJobKeyExchangeCalcPubValAlgorithmSecondaryFamily          |    |              |
| <b>Parent Container</b>          | CsmJobKeyExchangeCalcPubValConfig                            |    |              |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. |    |              |
| <b>Multiplicity</b>              | 1  |    |              |
| <b>Type</b>                      | EcucEnumerationParamDef                                      |    |              |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM  |    | 0xFF         |
|                                  | CRYPTO_ALGOFAM_NOT_SET                                       |    | 0x00         |
| <b>Post-Build Variant Value</b>  | false  |    |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>                                      | X  | All Variants |
|                                  | <b>Link time</b>   | -- |              |
|                                  | <b>Post-build time</b>                                       | -- |              |
| <b>Scope / Dependency</b>        | scope: local   |    |              |

|                         |  |  |  |
|-------------------------|--|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00232 :</b>  |  |  |
| <b>Name</b>             | CsmJobKeyExchangeCalcPubValAlgorithmSecondaryFamilyCustom                                  |  |  |
| <b>Parent Container</b> | CsmJobKeyExchangeCalcPubValConfig  |  |  |
| <b>Description</b>      | This is the second name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used . |  |  |
| <b>Multiplicity</b>     | 0..1   |  |  |
| <b>Type</b>             | EcucStringParamDef   |  |  |
| <b>Default value</b>    | --   |  |  |



|   |                         |    |              |
|---|-------------------------|----|--------------|
| <b>maxLength</b>                        | --                      |    |              |
| <b>minLength</b>                        | --                      |    |              |
| <b>regularExpression</b>                | --                      |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false                   |    |              |
| <b>Post-Build Variant Value</b>         | false                   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b> | X  | All Variants |
|   | <b>Link time</b>        | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local            |    |              |

**No Included Containers**

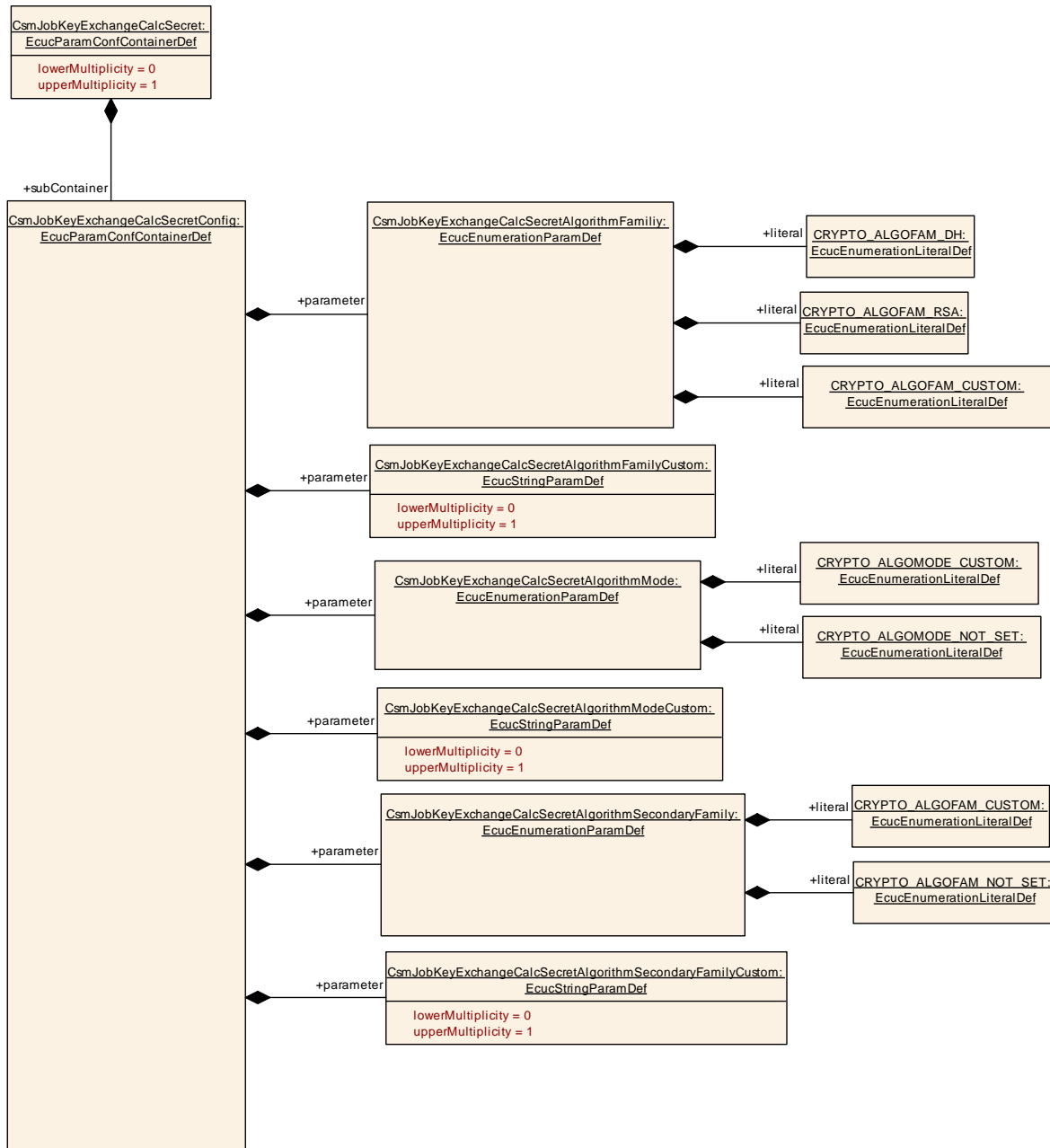


Figure 9-23 CsmJobKeyExchangeCalcSecret Layout

10.2.42 CsmJobKeyExchangeCalcSecret

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00201 :</b>                            |
| <b>Container Name</b>           | CsmJobKeyExchangeCalcSecret                        |
| <b>Parent Container</b>         | CsmPrimitives                                      |
| <b>Description</b>              | Configurations of KeyExchangeCalcSecret primitives |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b>        |                     |   |
|-----------------------------------|---------------------|---|
| <b>Container Name</b>             | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CsmJobKeyExchangeCalcSecretConfig | 1                   | Container for configuration of a CSM JobKeyExchangeCalcSecret. The container name serves as a symbolic name for the identifier of a |

|  |   |
|--|---|
|  | JobKeyExchangeCalcSecret configuration. |
|--|---|

### 10.2.43 CsmJobKeyExchangeCalcSecretConfig

|                                 |   |  |  |
|---------------------------------|---|--|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00234 :</b>   |  |  |
| <b>Container Name</b>           | CsmJobKeyExchangeCalcSecretConfig   |  |  |
| <b>Parent Container</b>         | CsmJobKeyExchangeCalcSecret   |  |  |
| <b>Description</b>              | Container for configuration of a CSM JobKeyExchangeCalcSecret. The container name serves as a symbolic name for the identifier of a JobKeyExchangeCalcSecret configuration. |  |  |
| <b>Configuration Parameters</b> |   |  |  |

|                                  |   |      |              |
|----------------------------------|---|------|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00235 :</b>   |      |              |
| <b>Name</b>                      | CsmJobKeyExchangeCalcSecretAlgorithmFamiliy   |      |              |
| <b>Parent Container</b>          | CsmJobKeyExchangeCalcSecretConfig   |      |              |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. This parameter defines the most significant part of the algorithm. |      |              |
| <b>Multiplicity</b>              | 1   |      |              |
| <b>Type</b>                      | EcucEnumerationParamDef   |      |              |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM   | 0xFF |              |
|                                  | CRYPTO_ALGOFAM_DH   | 0x26 |              |
|                                  | CRYPTO_ALGOFAM_RSA  | 0x13 |              |
| <b>Post-Build Variant Value</b>  | false   |      |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>   | X    | All Variants |
|                                  | <b>Link time</b>  | --   |              |
|                                  | <b>Post-build time</b>  | --   |              |
| <b>Scope / Dependency</b>        | scope: local  |      |              |

|   |   |    |              |
|---|---|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00236 :</b>   |    |              |
| <b>Name</b>                             | CsmJobKeyExchangeCalcSecretAlgorithmFamilyCustom  |    |              |
| <b>Parent Container</b>                 | CsmJobKeyExchangeCalcSecretConfig   |    |              |
| <b>Description</b>                      | Name of the custom algorithm family used for the crypto service. This is the name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

|                                  |   |    |              |
|----------------------------------|---|----|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00237 :</b>                                   |    |              |
| <b>Name</b>                      | CsmJobKeyExchangeCalcSecretAlgorithmMode                  |    |              |
| <b>Parent Container</b>          | CsmJobKeyExchangeCalcSecretConfig                         |    |              |
| <b>Description</b>               | Determines the algorithm mode used for the crypto service |    |              |
| <b>Multiplicity</b>              | 1   |    |              |
| <b>Type</b>                      | EcucEnumerationParamDef                                   |    |              |
| <b>Range</b>                     | CRYPTO_ALGOMODE_CUSTOM                                    |    | 0xFF         |
|                                  | CRYPTO_ALGOMODE_NOT_SET                                   |    | 0x00         |
| <b>Post-Build Variant Value</b>  | false   |    |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>                                   | X  | All Variants |
|                                  | <b>Link time</b>  | -- |              |
|                                  | <b>Post-build time</b>                                    | -- |              |
| <b>Scope / Dependency</b>        | scope: local  |    |              |

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00238 :</b>                        |    |              |
| <b>Name</b>                             | CsmJobKeyExchangeCalcSecretAlgorithmModeCustom |    |              |
| <b>Parent Container</b>                 | CsmJobKeyExchangeCalcSecretConfig              |    |              |
| <b>Description</b>                      | Name of the custom primitive mode.             |    |              |
| <b>Multiplicity</b>                     | 0..1   |    |              |
| <b>Type</b>                             | EcucStringParamDef                             |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false  |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                        | X  | All Variants |
|   | <b>Link time</b>                               | -- |              |
|   | <b>Post-build time</b>                         | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>                        | X  | All Variants |
|   | <b>Link time</b>                               | -- |              |
|   | <b>Post-build time</b>                         | -- |              |
| <b>Scope / Dependency</b>               | scope: local                                   |    |              |

|                                  |  |    |              |
|----------------------------------|--|----|--------------|
| <b>SWS Item</b>                  | <b>ECUC_Csm_00239 :</b>                                      |    |              |
| <b>Name</b>                      | CsmJobKeyExchangeCalcSecretAlgorithmSecondaryFamily          |    |              |
| <b>Parent Container</b>          | CsmJobKeyExchangeCalcSecretConfig                            |    |              |
| <b>Description</b>               | Determines the algorithm family used for the crypto service. |    |              |
| <b>Multiplicity</b>              | 1  |    |              |
| <b>Type</b>                      | EcucEnumerationParamDef                                      |    |              |
| <b>Range</b>                     | CRYPTO_ALGOFAM_CUSTOM  |    | 0xFF         |
|                                  | CRYPTO_ALGOFAM_NOT_SET                                       |    | 0x00         |
| <b>Post-Build Variant Value</b>  | false  |    |              |
| <b>Value Configuration Class</b> | <b>Pre-compile time</b>                                      | X  | All Variants |
|                                  | <b>Link time</b>   | -- |              |
|                                  | <b>Post-build time</b>                                       | -- |              |
| <b>Scope / Dependency</b>        | scope: local   |    |              |

|                         |   |  |  |
|-------------------------|---|--|--|
| <b>SWS Item</b>         | <b>ECUC_Csm_00240 :</b>                                   |  |  |
| <b>Name</b>             | CsmJobKeyExchangeCalcSecretAlgorithmSecondaryFamilyCustom |  |  |
| <b>Parent Container</b> | CsmJobKeyExchangeCalcSecretConfig                         |  |  |

|   |   |    |              |
|---|---|----|--------------|
| <b>Description</b>                      | This is the second name of the custom algorithm family, if CRYPTO_ALGOFAM_CUSTOM is used. |    |              |
| <b>Multiplicity</b>                     | 0..1  |    |              |
| <b>Type</b>                             | EcucStringParamDef  |    |              |
| <b>Default value</b>                    | --  |    |              |
| <b>maxLength</b>                        | --  |    |              |
| <b>minLength</b>                        | --  |    |              |
| <b>regularExpression</b>                | --  |    |              |
| <b>Post-Build Variant Multiplicity</b>  | false   |    |              |
| <b>Post-Build Variant Value</b>         | false   |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>   | X  | All Variants |
|   | <b>Link time</b>  | -- |              |
|   | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b>               | scope: local  |    |              |

**No Included Containers**

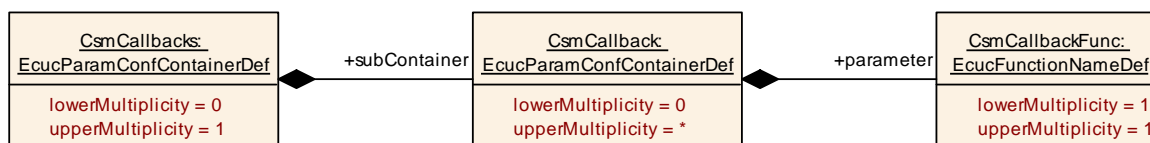


Figure 9-24 CsmCallbacks Layout

### 10.2.44 CsmCallbacks

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>ECUC_Csm_00008 :</b>                        |
| <b>Container Name</b>           | CsmCallbacks                                   |
| <b>Parent Container</b>         | Csm  |
| <b>Description</b>              | Container for callback function configurations |
| <b>Configuration Parameters</b> |  |

| <b>Included Containers</b> |                     |  |
|----------------------------|---------------------|--|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                          |
| CsmCallback                | 0..*                | Container for configuration of a callback function |

### 10.2.45 CsmCallback

|   |  |    |              |
|---|--|----|--------------|
| <b>SWS Item</b>                         | <b>ECUC_Csm_00109 :</b>                            |    |              |
| <b>Container Name</b>                   | CsmCallback  |    |              |
| <b>Parent Container</b>                 | CsmCallbacks                                       |    |              |
| <b>Description</b>                      | Container for configuration of a callback function |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>                            | X  | All Variants |
|   | <b>Link time</b>                                   | -- |              |
|   | <b>Post-build time</b>                             | -- |              |

**Configuration Parameters**

| <b>SWS Item</b>                         |  |    |              |
|---|--|----|--------------|
| <b>ECUC_Csm_00110 :</b>                 |  |    |              |
| <b>Name</b>                             | CsmCallbackFunc  |    |              |
| <b>Parent Container</b>                 | CsmCallback  |    |              |
| <b>Description</b>                      | Callback function to be called if an asynchronous operation has finished. The corresponding job has to be configured to be processed asynchronously. |    |              |
| <b>Multiplicity</b>                     | 1  |    |              |
| <b>Type</b>                             | EcucFunctionNameDef  |    |              |
| <b>Default value</b>                    | --   |    |              |
| <b>maxLength</b>                        | --   |    |              |
| <b>minLength</b>                        | --   |    |              |
| <b>regularExpression</b>                | --   |    |              |
| <b>Post-Build Variant Value</b>         | false  |    |              |
| <b>Multiplicity Configuration Class</b> | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Value Configuration Class</b>        | <b>Pre-compile time</b>  | X  | All Variants |
|   | <b>Link time</b>   | -- |              |
|   | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b>               | scope: local   |    |              |

**No Included Containers**

### 10.3 Published Information

For details refer to the chapter 10.3 “Published Information” in *SWS\_BSWGeneral*.