

|                                   |   |
|-----------------------------------|---|
| <b>Document Title</b>             | Specification of Crypto Abstraction Library |
| <b>Document Owner</b>             | AUTOSAR                                     |
| <b>Document Responsibility</b>    | AUTOSAR                                     |
| <b>Document Identification No</b> | 438   |
| <b>Document Classification</b>    | Standard                                    |

|                         |       |
|-------------------------|-------|
| <b>Document Version</b> | 1.2.0 |
| <b>Document Status</b>  | Final |
| <b>Part of Release</b>  | 4.0   |
| <b>Revision</b>         | 3     |

| <b>Document Change History</b> |                |                        |   |
|--------------------------------|----------------|------------------------|---|
| <b>Date</b>                    | <b>Version</b> | <b>Changed by</b>      | <b>Change Description</b>   |
| 12.12.2011                     | 1.2.0          | AUTOSAR Administration | <ul style="list-style-type: none"><li>• CAL0707 and CAL0708_Conf have been removed and the key types structures (e.g. Cal_AsymPrivateKeyType) now explicitly can contain a key handle instead of key data</li></ul>   |
| 24.11.2010                     | 1.1.0          | AUTOSAR Administration | <ul style="list-style-type: none"><li>• Integration of key transport services</li><li>• Key derivation output lenght specified through a parameter</li><li>• Remove descriptions that reference TRNGs</li><li>• Complete Configuration parameters</li></ul> |
| 30.11.2009                     | 1.0.0          | AUTOSAR Administration | Initial release   |

## Disclaimer

This specification 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 specification.

The material contained in this specification is protected by copyright and other types of Intellectual Property Rights. The commercial exploitation of the material contained in this specification requires a license to such Intellectual Property Rights.

This specification 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 specification may be utilized or reproduced, in any form or by any means, without permission in writing from the publisher.

The AUTOSAR specifications have been developed for automotive applications only. They have neither been developed, nor tested for non-automotive applications.

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

## Advice for users

AUTOSAR Specification Documents may contain exemplary items (exemplary reference models, "use cases", and/or references to exemplary technical solutions, devices, processes or software).

Any such exemplary items are contained in the Specification Documents for illustration purposes only, and they themselves are not part of the AUTOSAR Standard. Neither their presence in such Specification Documents, nor any later documentation of AUTOSAR conformance of products actually implementing such exemplary items, imply that intellectual property rights covering such exemplary items are licensed under the same rules as applicable to the AUTOSAR Standard.

## Table of Contents

|         |   |    |
|---------|---|----|
| 1       | Introduction and functional overview .....                    | 8  |
| 2       | Acronyms and abbreviations .....                              | 9  |
| 3       | Related documentation.....                                    | 10 |
| 3.1     | Input documents.....  | 10 |
| 3.2     | Related standards and norms .....                             | 10 |
| 4       | Constraints and assumptions .....                             | 11 |
| 4.1     | Limitations .....   | 11 |
| 4.2     | Applicability to car domains.....                             | 11 |
| 5       | Dependencies to other modules.....                            | 12 |
| 5.1     | File structure .....  | 12 |
| 5.1.1   | Code file structure .....                                     | 12 |
| 5.1.2   | Header file structure.....                                    | 12 |
| 6       | Requirements traceability .....                               | 15 |
| 6.1     | Document: Requirements on Libraries .....                     | 15 |
| 6.2     | Document: AUTOSAR requirements on Basic Software, general ... | 15 |
| 6.3     | Document: Requirements on CSM.....                            | 16 |
| 7       | Functional specification .....                                | 18 |
| 7.1     | Basic architecture guidelines.....                            | 18 |
| 7.2     | General behavior.....   | 18 |
| 7.2.1   | Configuration.....  | 18 |
| 7.2.2   | Normal operation.....   | 19 |
| 7.2.2.1 | Initialization and shutdown .....                             | 19 |
| 7.2.2.2 | Streaming Approach.....                                       | 19 |
| 7.2.2.3 | Context of services.....                                      | 22 |
| 7.3     | Version check.....  | 22 |
| 7.4     | Error detection.....  | 23 |
| 7.5     | Error notification .....                                      | 24 |
| 7.6     | Using Library API .....                                       | 24 |
| 7.7     | Library implementation .....                                  | 25 |
| 8       | API specification .....                                       | 27 |
| 8.1     | Imported types .....  | 27 |
| 8.2     | Type definitions .....  | 27 |
| 8.2.1   | API types.....  | 27 |
| 8.2.1.1 | Cal_ReturnType .....  | 27 |
| 8.2.1.2 | Cal_ConfigIdType.....   | 27 |
| 8.2.1.3 | Cal_<Service>ConfigType .....                                 | 28 |
| 8.2.1.4 | Cal_AlignType .....   | 28 |
| 8.2.1.5 | Cal_<Service>CtxBufType .....                                 | 29 |
| 8.2.1.6 | Cal_VerifyResultType.....                                     | 29 |
| 8.2.1.7 | Cal_AsymPublicKeyType .....                                   | 29 |
| 8.2.1.8 | Cal_AsymPrivateKeyType.....                                   | 30 |

|          |                                     |    |
|----------|-------------------------------------|----|
| 8.2.1.9  | Cal_SymKeyType .....                | 30 |
| 8.2.1.10 | Cal_KeyExchangeBaseType .....       | 30 |
| 8.2.1.11 | Cal_KeyExchangePrivateKeyType ..... | 31 |
| 8.3      | API functions .....                 | 31 |
| 8.3.1    | General interfaces .....            | 31 |
| 8.3.1.1  | Cal_GetVersionInfo .....            | 31 |
| 8.3.2    | Hash interface .....                | 32 |
| 8.3.2.1  | Cal_HashStart .....                 | 32 |
| 8.3.2.2  | Cal_HashUpdate .....                | 33 |
| 8.3.2.3  | Cal_HashFinish .....                | 33 |
| 8.3.3    | MAC interface .....                 | 34 |
| 8.3.3.1  | Cal_MacGenerateStart .....          | 35 |
| 8.3.3.2  | Cal_MacGenerateUpdate .....         | 35 |
| 8.3.3.3  | Cal_MacGenerateFinish .....         | 36 |
| 8.3.3.4  | Cal_MacVerifyStart .....            | 37 |
| 8.3.3.5  | Cal_MacVerifyUpdate .....           | 38 |
| 8.3.3.6  | Cal_MacVerifyFinish .....           | 38 |
| 8.3.4    | Random interface .....              | 39 |
| 8.3.4.1  | Cal_RandomSeedStart .....           | 39 |
| 8.3.4.2  | Cal_RandomSeedUpdate .....          | 40 |
| 8.3.4.3  | Cal_RandomSeedFinish .....          | 40 |
| 8.3.4.4  | Cal_RandomGenerate .....            | 41 |
| 8.3.5    | Symmetrical block interface .....   | 42 |
| 8.3.5.1  | Cal_SymBlockEncryptStart .....      | 42 |
| 8.3.5.2  | Cal_SymBlockEncryptUpdate .....     | 43 |
| 8.3.5.3  | Cal_SymBlockEncryptFinish .....     | 44 |
| 8.3.5.4  | Cal_SymBlockDecryptStart .....      | 45 |
| 8.3.5.5  | Cal_SymBlockDecryptUpdate .....     | 45 |
| 8.3.5.6  | Cal_SymBlockDecryptFinish .....     | 46 |
| 8.3.6    | Symmetrical interface .....         | 47 |
| 8.3.6.1  | Cal_SymEncryptStart .....           | 47 |
| 8.3.6.2  | Cal_SymEncryptUpdate .....          | 48 |
| 8.3.6.3  | Cal_SymEncryptFinish .....          | 49 |
| 8.3.6.4  | Cal_SymDecryptStart .....           | 50 |
| 8.3.6.5  | Cal_SymDecryptUpdate .....          | 51 |
| 8.3.6.6  | Cal_SymDecryptFinish .....          | 52 |
| 8.3.7    | Asymmetrical interface .....        | 53 |
| 8.3.7.1  | Cal_AsymEncryptStart .....          | 53 |
| 8.3.7.2  | Cal_AsymEncryptUpdate .....         | 53 |
| 8.3.7.3  | Cal_AsymEncryptFinish .....         | 54 |
| 8.3.7.4  | Cal_AsymDecryptStart .....          | 55 |
| 8.3.7.5  | Cal_AsymDecryptUpdate .....         | 56 |
| 8.3.7.6  | Cal_AsymDecryptFinish .....         | 57 |
| 8.3.8    | Signature interface .....           | 58 |
| 8.3.8.1  | Cal_SignatureGenerateStart .....    | 58 |
| 8.3.8.2  | Cal_SignatureGenerateUpdate .....   | 59 |
| 8.3.8.3  | Cal_SignatureGenerateFinish .....   | 59 |
| 8.3.8.4  | Cal_SignatureVerifyStart .....      | 60 |
| 8.3.8.5  | Cal_SignatureVerifyUpdate .....     | 61 |
| 8.3.8.6  | Cal_SignatureVerifyFinish .....     | 62 |

|          |   |    |
|----------|---|----|
| 8.3.9    | Checksum interface.....                                   | 62 |
| 8.3.9.1  | Cal_ChecksumStart .....                                   | 63 |
| 8.3.9.2  | Cal_ChecksumUpdate .....                                  | 63 |
| 8.3.9.3  | Cal_ChecksumFinish .....                                  | 64 |
| 8.3.10   | Key derivation interface.....                             | 65 |
| 8.3.10.1 | Cal_KeyDeriveStart.....                                   | 65 |
| 8.3.10.2 | Cal_KeyDeriveUpdate .....                                 | 66 |
| 8.3.10.3 | Cal_KeyDeriveFinish .....                                 | 67 |
| 8.3.11   | Key exchange interface.....                               | 67 |
| 8.3.11.1 | Cal_KeyExchangeCalcPubVal .....                           | 68 |
| 8.3.11.2 | Cal_KeyExchangeCalcSecretStart.....                       | 68 |
| 8.3.11.3 | Cal_KeyExchangeCalcSecretUpdate .....                     | 69 |
| 8.3.11.4 | Cal_KeyExchangeCalcSecretFinish .....                     | 70 |
| 8.3.12   | Symmetrical key extract interface .....                   | 71 |
| 8.3.12.1 | Cal_SymKeyExtractStart .....                              | 71 |
| 8.3.12.2 | Cal_SymKeyExtractUpdate .....                             | 72 |
| 8.3.12.3 | Cal_SymKeyExtractFinish .....                             | 73 |
| 8.3.13   | Symmetrical key wrapping interface.....                   | 73 |
| 8.3.13.1 | Cal_SymKeyWrapSymStart .....                              | 73 |
| 8.3.13.2 | Cal_SymKeyWrapSymUpdate .....                             | 74 |
| 8.3.13.3 | Cal_SymKeyWrapSymFinish .....                             | 75 |
| 8.3.13.4 | Cal_SymKeyWrapAsymStart.....                              | 76 |
| 8.3.13.5 | Cal_SymKeyWrapAsymUpdate.....                             | 76 |
| 8.3.13.6 | Cal_SymKeyWrapAsymFinish.....                             | 77 |
| 8.3.14   | Asymmetrical key extract interfaces .....                 | 78 |
| 8.3.14.1 | Cal_AsymPublicKeyExtractStart .....                       | 78 |
| 8.3.14.2 | Cal_AsymPublicKeyExtractUpdate .....                      | 78 |
| 8.3.14.3 | Cal_AsymPublicKeyExtractFinish .....                      | 79 |
| 8.3.14.4 | Cal_AsymPrivateKeyExtractStart .....                      | 80 |
| 8.3.14.5 | Cal_AsymPrivateKeyExtractUpdate .....                     | 80 |
| 8.3.14.6 | Cal_AsymPrivateKeyExtractFinish .....                     | 81 |
| 8.3.15   | Asymmetrical key wrapping interface .....                 | 82 |
| 8.3.15.1 | Cal_AsymPrivateKeyWrapSymStart .....                      | 82 |
| 8.3.15.2 | Cal_AsymPrivateKeyWrapSymUpdate .....                     | 83 |
| 8.3.15.3 | Cal_AsymPrivateKeyWrapSymFinish .....                     | 83 |
| 8.3.15.4 | Cal_AsymPrivateKeyWrapAsymStart.....                      | 84 |
| 8.3.15.5 | Cal_AsymPrivateKeyWrapAsymUpdate.....                     | 85 |
| 8.3.15.6 | Cal_AsymPrivateKeyWrapAsymFinish.....                     | 86 |
| 8.4      | Dependencies to cryptographic library API functions ..... | 86 |
| 8.4.1    | Types for the Cryptographic Primitives.....               | 86 |
| 8.4.1.1  | Cpl_<Primitive>ConfigType.....                            | 86 |
| 8.4.2    | API functions of the cryptographic primitives.....        | 87 |
| 8.4.2.1  | Cpl_<Primitive>Start .....                                | 87 |
| 8.4.2.2  | Cpl_<Primitive>Update .....                               | 87 |
| 8.4.2.3  | Cpl_<Primitive>Finish .....                               | 88 |
| 8.4.2.4  | Cpl_<Primitive> .....                                     | 89 |
| 8.4.3    | Configuration of the cryptographic primitives .....       | 90 |
| 9        | Sequence diagrams .....                                   | 91 |
| 10       | Configuration .....                                       | 92 |

|         |  |     |
|---------|--|-----|
| 10.1    | How to read this chapter .....                   | 92  |
| 10.1.1  | Configuration and configuration parameters ..... | 92  |
| 10.1.2  | Variants .....                                   | 93  |
| 10.1.3  | Containers .....                                 | 93  |
| 10.2    | Containers and configuration parameters .....    | 93  |
| 10.2.1  | Variants .....                                   | 93  |
| 10.2.2  | Cal .....  | 93  |
| 10.2.3  | CalGeneral .....                                 | 94  |
| 10.2.4  | CalHash .....                                    | 94  |
| 10.2.5  | CalHashConfig .....                              | 95  |
| 10.2.6  | CalMacGenerate .....                             | 96  |
| 10.2.7  | CalMacGenerateConfig .....                       | 96  |
| 10.2.8  | CalMacVerify .....                               | 97  |
| 10.2.9  | CalMacVerifyConfig .....                         | 98  |
| 10.2.10 | CalRandomSeed .....                              | 99  |
| 10.2.11 | CalRandomSeedConfig .....                        | 99  |
| 10.2.12 | CalRandomGenerate .....                          | 100 |
| 10.2.13 | CalRandomGenerateConfig .....                    | 100 |
| 10.2.14 | CalSymBlockEncrypt .....                         | 101 |
| 10.2.15 | CalSymBlockEncryptConfig .....                   | 102 |
| 10.2.16 | CalSymBlockDecrypt .....                         | 102 |
| 10.2.17 | CalSymBlockDecryptConfig .....                   | 103 |
| 10.2.18 | CalSymEncrypt .....                              | 104 |
| 10.2.19 | CalSymEncryptConfig .....                        | 105 |
| 10.2.20 | CalSymDecrypt .....                              | 105 |
| 10.2.21 | CalSymDecryptConfig .....                        | 106 |
| 10.2.22 | CalAsymEncrypt .....                             | 107 |
| 10.2.23 | CalAsymEncryptConfig .....                       | 108 |
| 10.2.24 | CalAsymDecrypt .....                             | 108 |
| 10.2.25 | CalAsymDecryptConfig .....                       | 109 |
| 10.2.26 | CalSignatureGenerate .....                       | 110 |
| 10.2.27 | CalSignatureGenerateConfig .....                 | 111 |
| 10.2.28 | CalSignatureVerify .....                         | 111 |
| 10.2.29 | CalSignatureVerifyConfig .....                   | 112 |
| 10.2.30 | CalChecksum .....                                | 113 |
| 10.2.31 | CalChecksumConfig .....                          | 113 |
| 10.2.32 | CalKeyDerive .....                               | 114 |
| 10.2.33 | CalKeyDeriveConfig .....                         | 115 |
| 10.2.34 | CalKeyExchangeCalcPubVal .....                   | 116 |
| 10.2.35 | CalKeyExchangeCalcPubValConfig .....             | 117 |
| 10.2.36 | CalKeyExchangeCalcSecret .....                   | 117 |
| 10.2.37 | CalKeyExchangeCalcSecretConfig .....             | 118 |
| 10.2.38 | CalSymKeyExtract .....                           | 119 |
| 10.2.39 | CalSymKeyExtractConfig .....                     | 120 |
| 10.2.40 | CalAsymPublicKeyExtract .....                    | 121 |
| 10.2.41 | CalAsymPublicKeyExtractConfig .....              | 121 |
| 10.2.42 | CalAsymPrivateKeyExtract .....                   | 122 |
| 10.2.43 | CalAsymPrivateKeyExtractConfig .....             | 123 |
| 10.2.44 | CalSymKeyWrapAsym .....                          | 124 |
| 10.2.45 | CalSymKeyWrapAsymConfig .....                    | 124 |

|         |                                       |     |
|---------|---------------------------------------|-----|
| 10.2.46 | CalSymKeyWrapSym.....                 | 125 |
| 10.2.47 | CalSymKeyWrapSymConfig .....          | 126 |
| 10.2.48 | CalAsymPrivateKeyWrapAsym .....       | 126 |
| 10.2.49 | CalAsymPrivateKeyWrapAsymConfig ..... | 127 |
| 10.2.50 | CalAsymPrivateKeyWrapSym .....        | 128 |
| 10.2.51 | CalAsymPrivateKeyWrapSymConfig .....  | 129 |
| 10.3    | Published Information.....            | 130 |
| 11      | Not applicable requirements .....     | 131 |

## 1 Introduction and functional overview

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

The CAL shall provide synchronous services to enable a unique access to basic cryptographic functionalities for all software modules and software components. The functionality required by a software module/component can be different to the functionality required by other software modules/components. For this reason there shall be the possibility to configure the services provided by the CAL individually for all software modules/components.

The construction of the CAL module follows a generic approach. Wherever a detailed specification of structures and interfaces would limit the scope of the usability of the CAL, 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 [\[10\]](#), are listed in this chapter.

| <b><i>Abbreviation /<br/>Acronym:</i></b> | <b><i>Description:</i></b>      |
|---|---------------------------------|
| CAL / Cal                                 | Crypto Abstraction Library      |
| CPL / Cpl                                 | Cryptographic Primitive Library |

## 3 Related documentation

### 3.1 Input documents

- [1] List of Basic Software Modules  
AUTOSAR\_TR\_BSWModuleList.pdf
- [2] AUTOSAR Layered Software Architecture  
AUTOSAR\_EXP\_LayeredSoftwareArchitecture.pdf
- [3] General Requirements on Basic Software Modules  
AUTOSAR\_SRS\_BSWGeneral.pdf
- [4] Specification of ECU Configuration  
AUTOSAR\_TPS\_ECUConfiguration.pdf
- [5] Specification of C Implementation Rules  
AUTOSAR\_TR\_CImplementationRules.pdf
- [6] Requirement on Libraries  
AUTOSAR\_SRS\_Libraries.pdf
- [7] Specification of Standard Types  
AUTOSAR\_SWS\_StandardTypes.pdf
- [8] Requirements on Crypto Service Manager  
AUTOSAR\_SRS\_CryptoServiceManager.pdf
- [9] Specification of Crypto Service Manager  
AUTOSAR\_SWS\_CryptoServiceManager.pdf
- [10] AUTOSAR Glossary  
AUTOSAR\_TR\_Glossary.pdf.pdf

### 3.2 Related standards and norms

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

## **4 Constraints and assumptions**

### **4.1 Limitations**

n.a.

### **4.2 Applicability to car domains**

n.a.

## 5 Dependencies to other modules

### [CAL0001]

┌ The CAL shall be able to incorporate cryptographic library modules, which are implemented according to the cryptographic library requirement specification in chapter 8.4. ┘()

### [CAL0506]

┌ The CAL shall use the interfaces of the incorporated cryptographic library modules to calculate the result of a cryptographic service.

The incorporated cryptographic library modules provide the implementation of cryptographic routines, e.g. MD5, SHA-1, RSA, AES, Diffie-Hellman key-exchange, etc. ┘()

## 5.1 File structure

### 5.1.1 Code file structure

#### [CAL0002]

┌ The code file structure shall not be defined within this specification completely. The CAL module shall consist of the following parts: ┘()

#### [ CAL0006]

┌ The code file structure shall contain one or more MISRA-C 2004 conform source files Cal\_<xxx>.c, that contain the entire parts of the CAL code. ┘(BSW007, BSW42600036)

#### [CAL0534]

┌ The code file structure shall contain one or more MISRA-C 2004 conform source files Cpl\_<xxx>.c, that contain the entire code of the incorporated cryptographic library modules. ┘(BSW007)

### 5.1.2 Header file structure

#### [CAL0535]

┌ The header file structure shall not be defined within this specification completely  
The CAL module shall provide the following headers: ┘()

**[CAL0005]**

┌ The header file structure shall contain an application interface header file Cal.h, that provides the function prototypes to access the CAL services. ┘(BSW31400005)

**[CAL0003]**

┌ The header file structure shall contain a configuration header Cal\_Cfg.h, that provides the configuration parameters for the CAL module. ┘()

**[CAL0004]**

┌ The header file structure shall contain a type header Cal\_Types.h, that provides the types, particularly configuration types, for the CAL module. ┘()

**[CAL0536]**

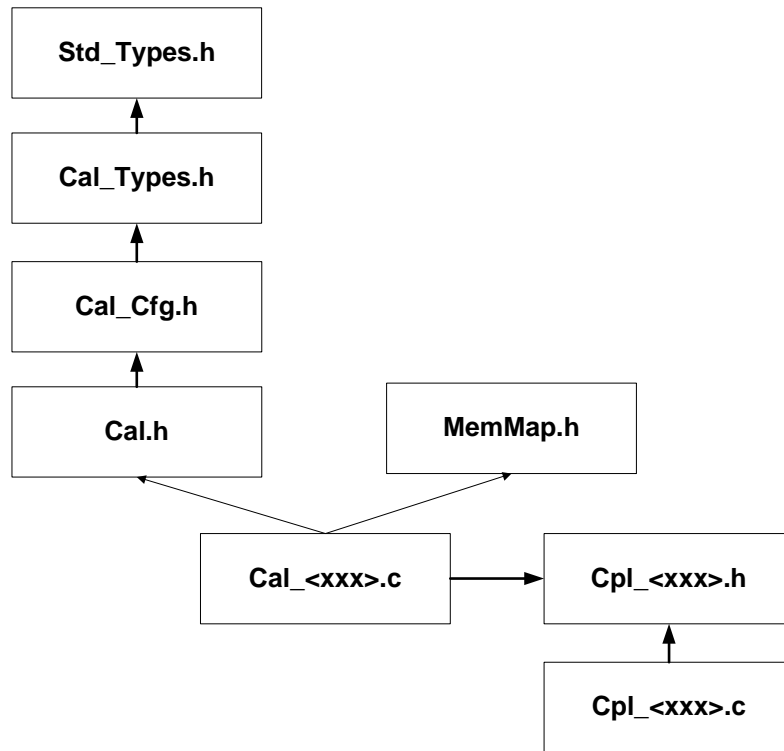
┌ Each underlying cryptographic library module shall provide a header file Cpl\_<xxx>.h. ┘()

**[CAL0008]**

┌ The Figure in CAL0537 (CAL File Structure) shows the include file structure, which shall be as follows:

- Cal\_Cfg.h shall include Cal\_Types.h.
- Cal\_Types.h shall include Std\_Types.h.
- Cal.h shall include Cal\_Cfg.h.
- Cal\_<xxx>.c shall include Cal.h and MemMap.h
- Cal\_<xxx>.c shall include Cpl\_<xxx>.h
- Cpl\_<xxx>.c shall include Cpl\_<xxx>.h ┘(BSW00348)

[CAL0537] 「



」()

## 6 Requirements traceability

### 6.1 Document: Requirements on Libraries

| <b>Requirement</b>  | <b>Satisfied by</b>   |
|---|---|
| [BSW31400001] The functional behavior of each library functions shall not be configurable | Chapter 10  |
| [BSW31400002] A library shall be operational before all BSW modules and application SWCs  | Chapter 7.2.2.1, CAL0021  |
| [BSW31400003] A library shall be operational until the shutdown                           | Chapter 7.2.2.1, CAL0027  |
| [BSW31400004] Using libraries shall not pass through a port interface                     | Chapter 7.7, CAL0731  |
| [BSW31400005] Library header file   | Section 5.1, CAL0005  |
| [BSW31400006] The header #include is placed by the SWC developer                          | Chapter 7.7, CAL0732  |
| [BSW31400007] Using a library should be documented  | Chapter 7.7, CAL0733  |
| [BSW31400008] Backward compatibility  | The SWS owner considers this requirement during future SWS evolution. |
| [BSW31400009] Re-entrancy   | All APIs in chapter 8 are defined to be re-entrant                    |
| [BSW31400010] Specific types  | Types are defined in chapter 8.                                       |
| [BSW31400011] Naming convention for functions and types                                   | APIs defined in chapter 8 are named according this requirement        |
| [BSW31400012] Passing parameters with structure is allowed                                | Some APIs in chapter 8 make use of this requirement.                  |
| [BSW31400013] Error detection   | Chapter 7.5, CAL0063, CAL0067   |
| [BSW31400015] Shared library code   | Chapter 7.8, CAL0734  |
| [BSW31400016] Non AUTOSAR library   | Not relevant. CAL is an AUTOSAR standard library                      |
| [BSW31400017] Usage of macros should be avoided   | Chapter 7.8, CAL0735  |
| [BSW31400018] A library function can only call library functions                          | Chapter 7.8, CAL0736  |

### 6.2 Document: AUTOSAR requirements on Basic Software, general

A library is not a basic software module. Therefore, many requirements for BSW modules are simply not applicable and not listed below. However, few requirements are relevant:

| <b>Requirement</b>  | <b>Satisfied by</b>          |
|---|------------------------------|
| [BSW00402] Published information  | Chapter 10.3, CAL0504        |
| [BSW00407] Function to read out published parameters                          | Chapter 8.3.1.1, CAL0705     |
| [BSW007] HIS MISRA C  | CAL0006, CAL0534, CAL0737    |
| [BSW00411] Get version info keyword   | Not applicable for libraries |
| [BSW00436] Module Header File Structure for the Basic Software Memory Mapping | CAL0008, CAL0738             |
| [BSW00348] Standard type header   | CAL0008, CAL0739             |
| [BSW00304] AUTOSAR integer data types   | Chapter 8, CAL0740           |
| [BSW00378] AUTOSAR boolean type   | Chapter 8, CAL0740           |
| [BSW00306] Avoid direct use of compiler and platform specific keywords        | CAL0741                      |
| [BSW00374] Module vendor identification                                       | Chapter 10.3, CAL0504        |
| [BSW00379] Module identification  | Chapter 10.3, CAL0504        |
| [BSW003] Version identification   | Chapter 10.3, CAL0504        |
| [BSW00318] Format of module version numbers                                   | Chapter 10.3, CAL0504        |
| [BSW00321] Enumeration of module version numbers                              | Chapter 10.3, CAL0504        |

### 6.3 Document: Requirements on CSM

| <b>Requirement</b>                             | <b>Satisfied by</b>                  |
|--|--------------------------------------|
| [BSW42600061] General interfaces               | Chapter 7.2                          |
| [BSW42600001] scalability                      | CAL0015                              |
| [BSW42600002] CRY interface                    | Chapter 8.4                          |
| [BSW42600069] CRY interface specification      | Chapter 8.4                          |
| [BSW42600010] role of cryptographic primitives | related to CSM, not relevant for CAL |
| [BSW42600011] internal CRY interface           | Chapter 8.4                          |
| [BSW42600004] configuration rules              | CAL0030                              |
| [BSW42600005] job processing mode              | related to CSM, not relevant for CAL |
| [BSW42600006] cryptographic services           | CAL0461                              |
| [BSW42600007] other modules                    | Chapter 5                            |
| [BSW42600008] callback function                | related to CSM, not relevant for CAL |
| [BSW42600009] initialization function          | related to CSM, not relevant for CAL |



|  |                                      |
|--|--------------------------------------|
| [BSW42600030] streaming approach               | CAL0023                              |
| [BSW42600063] streaming approach               | Chapter 8.4                          |
| [BSW42600012] error types                      | related to CSM, not relevant for CAL |
| [BSW42600013] development errors               | related to CSM, not relevant for CAL |
| [BSW42600014] development error codes via API  | related to CSM, not relevant for CAL |
| [BSW42600015] parameter checking               | related to CSM, not relevant for CAL |
| [BSW42600047] abstraction layer                | related to CSM, not relevant for CAL |
| [BSW42600064] location in service layer        | related to CSM, not relevant for CAL |
| [BSW42600068] RTE interface for callbacks      | related to CSM, not relevant for CAL |
| [BSW42600067] RTE interface for services       | related to CSM, not relevant for CAL |
| [BSW42600066] general RTE interface            | related to CSM, not relevant for CAL |
| [BSW42600060] configuration files              | Chapter 5.1                          |
| [BSW42600036] implementation                   | CAL0006                              |
| [BSW42600046] error and status information     | related to CSM, not relevant for CAL |
| [BSW42600056] files required                   | chapter 5.1                          |
| [BSW42600057] configuration and implementation | chapter 5.1                          |

## 7 Functional specification

### 7.1 Basic architecture guidelines

The AUTOSAR library CAL provides other BSW modules and application SWCs with cryptographic services.

The CAL offers C functions that can be called from source code, i.e. from BSW modules, from SWC or from Complex Device Drivers.

As the CAL is a library, it is not related to a special layer of the AUTOSAR Layered Software Architecture. The services of the CAL are always executed in the context of the calling function.

Many CRY/CPL<sup>1</sup> interfaces use the same cryptographic building blocks. Thus, cryptographic building blocks should be implemented as separate modules and be called from the CRY/CPL interfaces. This implies that the code for cryptographic building blocks should not be implemented more than once.

### 7.2 General behavior

#### [CAL0016]

┌ The CAL shall support reentrant access to all services. ┘(BSW31400009)

#### [CAL0022]

┌ The CAL shall allow parallel access to different services. ┘()

#### [CAL0035]

┌ The interface functions shall immediately compute the result, i.e they shall work synchronously. ┘()

#### 7.2.1 Configuration

#### [CAL0025]

┌ Each service configuration shall be realized as a constant structure of type Cal\_<Service>ConfigType . ┘()

#### [CAL0026]

┌ Each service configuration shall have a name which can be configured. ┘()

#### [CAL0028]

---

<sup>1</sup> CRY is defined by the Crypto Service Manager (see [8])

┌ It shall be possible to create arbitrary many service configurations for each cryptographic service. ┐()

**[CAL0029]**

┌ When creating a service configuration, it shall be possible to configure all available and allowed schemes and underlying cryptographic primitives. ┐()

**[CAL0030]**

┌ It shall be checked during configuration that only valid service configurations are chosen. ┐(BSW42600004)

**7.2.2 Normal operation****7.2.2.1 Initialization and shutdown****[CAL0021]**

┌ The CAL shall not require initialization phase. A Library function may be called at the very first step of ECU initialization, e.g. even by the OS or EcuM, thus the library shall be ready. ┐(BSW31400002)

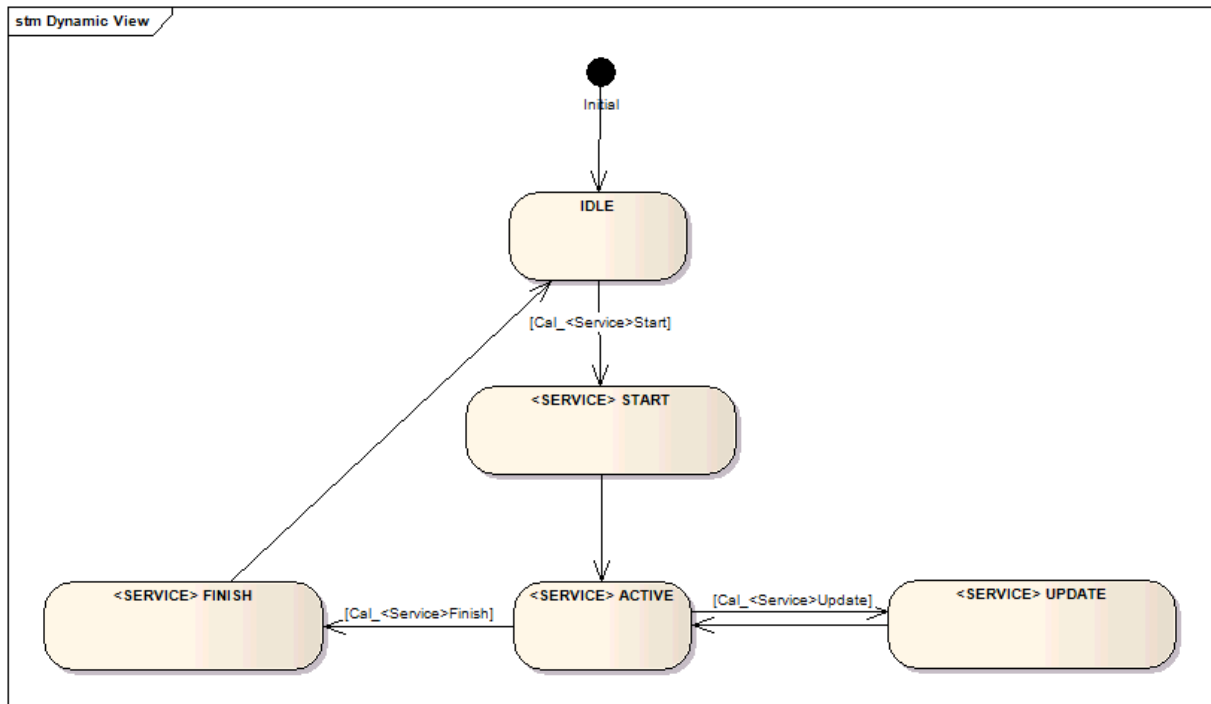
**[CAL0027]**

┌ The CAL shall not require a shutdown operation phase. ┐(BSW31400003)

**7.2.2.2 Streaming Approach****[CAL0023]**

┌ The implementation of those CAL services which expect arbitrary amounts of user data (i.e. the hashing or encryption service) shall be based on the streaming approach with start, update and finish functions. The diagram in CAL0024 shows the general design of such a CAL service. ┐(BSW42600030)

**[CAL0024]**  $\Uparrow$



$\Downarrow$ ()

**[CAL0728]**

$\Uparrow$  CAL services, which do not expect arbitrary amounts of user data, only have to provide an API `Cal_<Service>()` (e.g. `Cal_RandomGenerate`). These services shall be handled as simple function calls.  $\Downarrow$ ()

**[CAL0729]**

$\Uparrow$  CAL services, which expect arbitrary amounts of user data, shall provide the APIs `Cal_<Service>Start()`, `Cal_<Service>Update()` and `Cal_<Service>Finish()`. The communication between applications and these CAL services shall follow a strict sequence of steps which is described below. This ensures a reliable communication between applications and the CAL module.  $\Downarrow$ ()

All applications have to keep with the following rules:

**7.2.2.2.1 Initialization**

**[CAL0046]**

┌ The application calls the Cal\_<Service>Start request, passing a valid service configuration to the start function. The start function shall check the validity of the configuration it receives. ┘()

**[CAL0047]**

┌ Cal\_<Service>Start shall configure the CAL immediately, set the status of the current service to active, store the status of the service and all necessary context in the context buffer, and return. ┘()

**7.2.2.2.2 Update**

The application provides the data necessary for the computation of the intended service.

**[CAL0050]**

┌ The application calls the Cal\_<Service>Update request, passing data which is necessary for the computation of the service to the update function. The update function shall check whether the current service is already initialized. ┘()

**[CAL0051]**

┌ The CAL shall assume that the data provided to Cal\_<Service>Update will not change until it returns. ┘()

**[CAL0052]**

┌ If the service has been initialized before, the update function shall immediately process the given data, set the status of the current service again to active, store the status of the service and all necessary context in the context buffer, and return the status of the update. ┘()

**[CAL0054]**

┌ The CAL shall allow the application to call the update function arbitrarily often. ┘()

**7.2.2.2.3 Finish**

The application provides the result buffer necessary for the finishing of the computation of the intended service.

**[CAL0056]**

┌ The application calls the Cal\_<Service>Finish request, passing the result buffer and optional data which is necessary for the finishing of the cryptographic service to the finish function. The finish function shall check whether the current service is already initialized. 」（）

**[CAL0057]**

┌ The CAL shall assume that the data provided to Cal\_<Service>Finish will not change until it returns. 」（）

**[CAL0058]**

┌ If the service has been initialized before, the finish function shall immediately process the given data, finish the computation of the current cryptographic service, set the status of the service in the context buffer to idle, store the result of the service in the result buffer, and return the status of the finishing. 」（）

**7.2.2.3 Context of services**

As the CAL is a library, it is not allowed to store any internal states. When calling a service of the CAL, the application has to provide a pointer to a buffer, in which the CAL can store all context and status information that is necessary to process the service. This context buffer has to be provided consistently to all calls of the Start-, Update- and Finish-APIs belonging to one service request cycle.

**[CAL0730]**

┌ The size of the context buffer, that has to be provided by the caller, depends on the selected service and on the selected CPL method. The CAL part of the configuration tool shall generate a macro that contains the desired size of the context buffer for each service configuration. 」（）

All context buffers shall be aligned according to the maximum alignment of all scalar types on the given platform.

**7.3 Version check****[CAL0060]**

┌ The CAL module shall perform Inter Module Checks to avoid integration of incompatible files.

The imported included files shall be checked by preprocessing directives. 」（）

The following version numbers shall be verified:

- < MAB >\_AR\_RELEASE\_MAJOR\_VERSION
- < MAB >\_AR\_RELEASE\_MINOR\_VERSION

where <MAB> is the module module abbreviation of the other (external) modules which provide header files included by the CAL module.

If the values are not identical to the expected values, an error shall be reported.

## 7.4 Error detection

### [CAL0063]

「 Functions of the CAL should check at runtime (both in production and development code) the value of input parameters, especially cases where erroneous value can bring to fatal error or unpredictable result, if they have the values allowed by the function specification. All the error cases shall be listed in SWS and the function should return a specified value (in SWS) that is not configurable. This value is dependant of the function and the error case so it is determined case by case. 」  
(BSW31400013)

### [CAL0064]

「 The API parameters shall be checked in the order in which they are passed. 」()

### [CAL0488]

「 If an error is detected, the desired service shall return with CAL\_E\_NOT\_OK. 」()

### [CAL0489]

「 The following table specifies which errors shall be evaluated for each API call: 」()

### [CAL0539]

| API call                                  | Error condition                                   | API return value |
|---|---|------------------|
| All APIs that have a pointer as parameter | Pointer is Nullpointer                            | CAL_E_NOT_OK     |
| Cal_<Service>Update                       | Service is not initialized                        | CAL_E_NOT_OK     |
| Cal_<Service>Finish                       | Service is not initialized                        | CAL_E_NOT_OK     |
| Cal_<Service>Start                        | Invalid cryptographic method for selected service | CAL_E_NOT_OK     |
| Cal_<Service>                             | Invalid cryptographic method for selected service | CAL_E_NOT_OK     |
| Cal_MacGenerateStart                      | Invalid key type for selected service             | CAL_E_NOT_OK     |
| Cal_MacVerifyStart                        |   |                  |
| Cal_SymBlockEncryptStart                  |   |                  |

| API call                        | Error condition | API return value |
|---------------------------------|-----------------|------------------|
| Cal_SymBlockDecryptStart        |                 |                  |
| Cal_SymEncryptStart             |                 |                  |
| Cal_SymDecryptStart             |                 |                  |
| Cal_AsymEncryptStart            |                 |                  |
| Cal_AsymDecryptStart            |                 |                  |
| Cal_SigGenerateStart            |                 |                  |
| Cal_SigVerifyStart              |                 |                  |
| Cal_KeyDeriveStart              |                 |                  |
| Cal_KeyExchangeCalcPubVal       |                 |                  |
| Cal_KeyExchangeCalcSecretStart  |                 |                  |
| Cal_SymKeyExtractStart          |                 |                  |
| Cal_SymKeyWrapSymStart          |                 |                  |
| Cal_SymKeyWrapAsymStart         |                 |                  |
| Cal_AsymPrivateKeyExtractStart  |                 |                  |
| Cal_AsymPrivateKeyWrapSymStart  |                 |                  |
| Cal_AsymPrivateKeyWrapAsymStart |                 |                  |
| Cal_AsymPublicKeyExtractStart   |                 |                  |

」()

## 7.5 Error notification

### [CAL0067]

「 The functions of the CAL shall not call the DET in case of error. 」(BSW31400013)

## 7.6 Using Library API

### [CAL0731]

「 CAL API can be directly called from BSW modules or SWC. No port definition is required. It is a pure function call. 」(BSW31400004)

The statement `#include "Cal.h"` shall be placed by the developer or an application code generator but not by the RTE generator

### [CAL0733]



┌ Using a library shall be documented. If a BSW module or a SWC uses a Library, the developer shall add an Implementation-DependencyOnLibrary in the BSW/SWC template.

minVersion and maxVersion parameters correspond to the supplier version. In case of AUTOSAR library, these parameters may be left empty because a SWC or BSW module may rely on a library behaviour, not on a supplier implementation. However, the SWC or BSW modules shall be compatible with the AUTOSAR platform where they are integrated. ┘(BSW31400007)

## 7.7 Library implementation

### [CAL0015]

┌ Due to memory restrictions the CAL Library and the underlying Crypto Library shall only provide those services and algorithms which are necessary for the applications running on the ECU. Therefore parts of the CAL Library have to be generated based on a configuration that describes which cryptographic methods are necessary for the applications. ┘(BSW42600001)

### [CAL0734]

┌ The CAL shall be implemented in a way that the code can be shared among callers in different memory partitions. ┘(BSW31400015)

### [CAL0736]

┌ A library function shall not call any BSW modules functions. A library function can call other library functions. Because a library function shall be reentrant. But other BSW modules functions may not be reentrant. ┘(BSW31400018)

### [CAL0737]

┌ The library, written in C programming language, should conform to the HIS subset of the MISRA C Standard.

Only in technically reasonable, exceptional cases MISRA violations are permissible. Such violations against MISRA rules shall be clearly identified and documented within comments in the C source code (including rationale why MISRA rule is violated). The comment shall be placed right above the line of code which causes the violation and have the following syntax:

```
/* MISRA RULE XX VIOLATION: This the reason why the MISRA rule could not be followed in this special case*/ ┘(BSW007)
```

### [CAL0738]

┌ Each AUTOSAR library Module implementation <library>\*.c shall include the header file MemMap.h. ┘()

**[CAL0739]**

┐ Each AUTOSAR library Module implementation <library>\*.c, that uses AUTOSAR integer data types and/or the standard return, shall include the header file Std\_Types.h. ┘(BSW00348)

**[CAL0740]**

┐ All AUTOSAR library Modules should use the AUTOSAR data types (integers, boolean) instead of native C data types, unless this library is clearly identified to be compliant only with a platform. ┘(BSW00304, BSW00378)

**[CAL0741]**

┐ All AUTOSAR library Modules should avoid direct use of compiler and platform specific keyword, unless this library is clearly identified to be compliant only with a platform. ┘(BSW00306)

## 8 API specification

### 8.1 Imported types

#### [CAL0068]

「 Only the standard AUTOSAR types provided by Std\_Types.h shall be imported. 」()

### 8.2 Type definitions

#### 8.2.1 API types

##### 8.2.1.1 Cal\_ReturnType

#### [CAL0069] 「

|                     |  |  |
|---------------------|--|--|
| <b>Name:</b>        | Cal_ReturnType                                   |  |
| <b>Type:</b>        | Enumeration                                      |  |
| <b>Range:</b>       | CAL_E_OK   | The execution of the called function succeeded / the result of the called function is "ok".<br>This return code shall be given as value "0".             |
|                     | CAL_E_NOT_OK                                     | The execution of the called function failed / the result of the called function is "not ok".<br>This return code shall be given as value "1".            |
|                     | CAL_E_SMALL_BUFFER                               | The service request failed because the provided buffer is too small to store the result of the service.<br>This return code shall be given as value "3". |
|                     | CAL_E_ENTROPY_EXHAUSTION                         | The service request failed because the entropy of the random number generator is exhausted.<br>This return code shall be given as value "4".             |
| <b>Description:</b> | Enumeration of the return type of the CAL module |  |

」()

##### 8.2.1.2 Cal\_ConfigIdType

#### [CAL0073] 「

|                     |   |  |
|---------------------|---|--|
| <b>Name:</b>        | Cal_ConfigIdType  |  |
| <b>Type:</b>        | uint16  |  |
| <b>Description:</b> | Identification of a CAL service configuration via a numeric identifier that is unique within a service.   |  |
|                     | The name of a CAL service configuration, i.e. the name of the container Cal_<Service>Config, shall serve as a symbolic name for this parameter. |  |
|                     | Range: 0..65535   |  |

」()

### 8.2.1.3 Cal\_<Service>ConfigType

[CAL0074] ⌈

|                     |  |   |   |
|---------------------|--|---|---|
| <b>Name:</b>        | Cal_<Service>ConfigType  |   |   |
| <b>Type:</b>        | Structure  |   |   |
| <b>Element:</b>     | Cal_ConfigIdType   | ConfigId  | The numeric identifier of a configuration.  |
|                     | Cal_ReturnType   | (*PrimitiveStartFct)<br>(<primitive parameter list>)  | This element shall only exist if the service contains the function Cal_<Service>Start. It is a pointer to the function Cpl_<Primitive>Start of the configured cryptographic primitive. For the "primitive parameter list" see the description of Cpl_<Primitive>Start.    |
|                     | Cal_ReturnType   | (*PrimitiveUpdateFct)<br>(<primitive parameter list>) | This element shall only exist if the service contains the function Cal_<Service>Update. It is a pointer to the function Cpl_<Primitive>Update of the configured cryptographic primitive. For the "primitive parameter list" see the description of Cpl_<Primitive>Update. |
|                     | Cal_ReturnType   | (*PrimitiveFinishFct)<br>(<primitive parameter list>) | This element shall only exist if the service contains the function Cal_<Service>Finish. It is a pointer to the function Cpl_<Primitive>Finish of the configured cryptographic primitive. For the "primitive parameter list" see the description of Cpl_<Primitive>Finish. |
|                     | Cal_ReturnType   | (*PrimitiveFct)<br>(<primitive parameter list>)       | This element shall only exist if the service contains the function Cal_<Service>. It is a pointer to the function Cpl_<Primitive> of the configured cryptographic primitive. For the "primitive parameter list" see the description of Cpl_<Primitive>.                   |
|                     | void   | *PrimitiveConfigPtr                                   | A pointer to the configuration of the underlying cryptographic primitive  |
| <b>Description:</b> | Data structure which shall encompass all information needed to specify the cryptographic primitives needed for the <Service> cryptographic service. It shall furthermore contain information on the callback function. |   |   |

⌋()

### 8.2.1.4 Cal\_AlignType

[CAL0743] ⌈

|                     |  |
|---------------------|--|
| <b>Name:</b>        | Cal_AlignType  |
| <b>Type:</b>        | <maxAlignScalarType>   |
| <b>Description:</b> | A scalar type which has maximum alignment restrictions on the given platform. This value is configured by "CalMaxAlignScalarType". |

|  |  |
|--|--|
|  | <p>&lt;maxAlignScalarType&gt; can be e.g. uint8, uint16 or uint32.</p> <p>All context buffers shall be aligned according to the maximum alignment of all scalar types on the given platform.</p> |
|--|--|

()

### 8.2.1.5 Cal\_<Service>CtxBufType

[CAL0742] ⌈

|                     |   |
|---------------------|---|
| <b>Name:</b>        | Cal_<Service>CtxBufType   |
| <b>Type:</b>        | Cal_AlignType[CAL_<SERVICE>_CONTEXT_BUFFER_SIZE]  |
| <b>Description:</b> | <p>Type definition of the context buffer of a service.</p> <p>CAL_&lt;SERVICE&gt;_CONTEXT_BUFFER_SIZE shall be chosen such that "CAL_&lt;SERVICE&gt;_CONTEXT_BUFFER_SIZE * sizeof(Cal_AlignType)" is greater or equal "Cal&lt;Service&gt;MaxCtxBufferByteSize".</p> |

()

### 8.2.1.6 Cal\_VerifyResultType

[CAL0075] ⌈

|                     |  |   |  |
|---------------------|--|---|--|
| <b>Name:</b>        | Cal_VerifyResultType                                       |   |  |
| <b>Type:</b>        | Enumeration  |   |  |
| <b>Range:</b>       | CAL_E_VER_OK   | The result of the verification is "true", i.e. the two compared elements are identical.<br>This return code shall be given as value "0"       |  |
|                     | CAL_E_VER_NOT_OK   | The result of the verification is "false", i.e. the two compared elements are not identical.<br>This return code shall be given as value "1". |  |
| <b>Description:</b> | Enumeration of the result type of verification operations. |   |  |

()

### 8.2.1.7 Cal\_AsymPublicKeyType

[CAL0079] ⌈

|                     |  |        |  |
|---------------------|--|--------|--|
| <b>Name:</b>        | Cal_AsymPublicKeyType  |        |  |
| <b>Type:</b>        | Structure  |        |  |
| <b>Element:</b>     | uint32   | length | This element contains the length of the key stored in element 'data' |
|                     | Cal_AlignType<br>[CAL_ASYM_PUB_KEY_MAX_SIZE]   | data   | This element contains the key data or a key handle.                  |
| <b>Description:</b> | <p>Structure for the public asymmetrical key.</p> <p>CAL_ASYM_PUB_KEY_MAX_SIZE shall be chosen such that "CAL_ASYM_PUB_KEY_MAX_SIZE * sizeof(Cal_AlignType)" is greater or equal to the maximum of the configured values CalAsymEncryptMaxKeySize, CalSignatureVerifyMaxKeySize, CalAsymPublicKeyExtractMaxKeySize, CalSymKeyWrapAsymMaxPubKeySize and CalAsymPrivateKeyWrapAsymMaxPubKeySize.</p> |        |  |

()

### 8.2.1.8 Cal\_AsymPrivateKeyType

[CAL0080] ⌈

|                     |  |        |  |
|---------------------|--|--------|--|
| <b>Name:</b>        | Cal_AsymPrivateKeyType   |        |  |
| <b>Type:</b>        | Structure  |        |  |
| <b>Element:</b>     | uint32   | length | This element contains the length of the key stored in element 'data' |
|                     | Cal_AlignType[ CAL_ASYM_PRIV_KEY_MAX_SIZE]   | data   | This element contains the key data or a key handle.                  |
| <b>Description:</b> | Structure for the private asymmetrical key.<br>CAL_ASYM_PRIV_KEY_MAX_SIZE shall be chosen such that "CAL_ASYM_PRIV_KEY_MAX_SIZE * sizeof(Cal_AlignType)" is greater or equal to the maximum of the configured values CalAsymDecryptMaxKeySize, CalSignatureGenerateMaxKeySize, CalAsymPrivateKeyExtractMaxKeySize, CalAsymPrivateKeyWrapSymMaxPrivKeySize and CalAsymPrivateKeyWrapAsymMaxPrivKeySize. |        |  |

⌋()

### 8.2.1.9 Cal\_SymKeyType

[CAL0082] ⌈

|                     |  |        |  |
|---------------------|--|--------|--|
| <b>Name:</b>        | Cal_SymKeyType   |        |  |
| <b>Type:</b>        | Structure  |        |  |
| <b>Element:</b>     | uint32   | length | This element contains the length of the key stored in element 'data' |
|                     | Cal_AlignType[ CAL_SYM_KEY_MAX_SIZE]   | data   | This element contains the key data or a key handle.                  |
| <b>Description:</b> | Structure for the symmetrical key.<br>CAL_SYM_KEY_MAX_SIZE shall be chosen such that "CAL_SYM_KEY_MAX_SIZE * sizeof(Cal_AlignType)" is greater or equal to the maximum of the configured values CalSymBlockEncryptMaxKeySize, CalSymBlockDecryptMaxKeySize, CalSymEncryptMaxKeySize, CalSymDecryptMaxKeySize, CalKeyDeriveMaxKeySize, CalSymKeyExtractMaxKeySize, CalMacGenerateMaxKeySize, CalMacVerifyMaxKeySize, CalSymKeyWrapSymMaxSymKeySize, CalSymKeyWrapAsymMaxSymKeySize and CalAsymPrivateKeyWrapSymMaxSymKeySize. |        |  |

⌋()

### 8.2.1.10 Cal\_KeyExchangeBaseType

[CAL0086] ⌈

|                     |  |        |  |
|---------------------|--|--------|--|
| <b>Name:</b>        | Cal_KeyExchangeBaseType  |        |  |
| <b>Type:</b>        | Structure  |        |  |
| <b>Element:</b>     | uint32   | length | This element contains the length of the key stored in element 'data' |
|                     | Cal_AlignType [CAL_KEY_EX_BASE_MAX_SIZE]   | data   | This element contains the key data or a key handle.                  |
| <b>Description:</b> | Structure with base type information of the key exchange protocol.<br>CAL_KEY_EX_BASE_MAX_SIZE shall be chosen such that |        |  |

|  |  |
|--|--|
|  | "CAL_KEY_EX_BASE_MAX_SIZE * sizeof(Cal_AlignType)" is greater or equal to the maximum of the configured values CalKeyExchangeCalcPubValMaxBaseTypeSize and CalKeyExchangeCalcSecretMaxBaseTypeSize |
|--|--|

」()

### 8.2.1.11 Cal\_KeyExchangePrivateType

[CAL0087]「

|                     |   |        |  |
|---------------------|---|--------|--|
| <b>Name:</b>        | Cal_KeyExchangePrivateType  |        |  |
| <b>Type:</b>        | Structure   |        |  |
| <b>Element:</b>     | uint32  | length | This element contains the length of the key stored in element 'data' |
|                     | Cal_AlignType[CAL_KEY_EX_PRIV_MAX_SIZE]   | data   | This element contains the key data or a key handle.                  |
| <b>Description:</b> | Structure with the private Information of the key exchange protocol only known to the current user.<br>CAL_KEY_EX_PRIV_MAX_SIZE shall be chosen such that<br>"CAL_KEY_EX_PRIV_MAX_SIZE * sizeof(Cal_AlignType)" is greater or equal to the maximum of the configured values CalKeyExchangeCalcPubValMaxPrivateTypeSize and CalKeyExchangeCalcSecretMaxPrivateTypeSize |        |  |

」()

## 8.3 API functions

[CAL0478]

「 As the CAL is a library, all functions have to be reentrant. 」()

### 8.3.1 General interfaces

#### 8.3.1.1 Cal\_GetVersionInfo

[CAL0705]「

|                         |   |
|-------------------------|---|
| <b>Service name:</b>    | Cal_GetVersionInfo  |
| <b>Syntax:</b>          | void Cal_GetVersionInfo(<br>Std_VersionInfoType* versioninfo<br>) |
| <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>       | void  | none  |
| <b>Description:</b>        | Returns the version information of this module. |   |

\_(BSW00407)

#### [CAL0706]

▮ The function Cal\_GetVersionInfo shall return the version information of this module.

The version information includes:

- Module Id
- Vendor Id
- Vendor specific version numbers (BSW00407). \_()

### 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 Cal\_HashStart

##### [CAL0089] ▮

|                            |  |   |
|----------------------------|--|---|
| <b>Service name:</b>       | Cal_HashStart  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_HashStart(     Cal_ConfigIdType cfgId,     Cal_HashCtxBufType contextBuffer )</pre>  |   |
| <b>Service ID[hex]:</b>    | 0x03   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration that has to be used during the hash value computation. |
| <b>Parameters (inout):</b> | None   |   |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                         |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to initialize the hash service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |   |

\_()



Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_HashStart.

### 8.3.2.2 Cal\_HashUpdate

[CAL0094] ⌈

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_HashUpdate  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_HashUpdate(     Cal_ConfigIdType cfgId,     Cal_HashCtxBufType contextBuffer,     const uint8* dataPtr,     uint32 dataLength )</pre>   |   |
| <b>Service ID[hex]:</b>    | 0x04  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration that has to be used during the hash value computation. |
|                            | dataPtr   | Holds a pointer to the data to be hashed  |
|                            | dataLength  | Contains the number of bytes to be hashed.  |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                         |
| <b>Parameters (out):</b>   | None  |   |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to feed the hash service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The hash computation is done by the underlying primitive.</p> |   |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_HashUpdate.

### 8.3.2.3 Cal\_HashFinish

[CAL0101] ⌈

|                         |  |   |
|-------------------------|--|---|
| <b>Service name:</b>    | Cal_HashFinish   |   |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_HashFinish(     Cal_ConfigIdType cfgId,     Cal_HashCtxBufType contextBuffer,     uint8* resultPtr,     uint32* resultLengthPtr,     boolean TruncationIsAllowed )</pre> |   |
| <b>Service ID[hex]:</b> | 0x05   |   |
| <b>Sync/Async:</b>      | Synchronous  |   |
| <b>Reentrancy:</b>      | Reentrant  |   |
| <b>Parameters (in):</b> | cfgId  | Holds the identifier of the CAL module configuration that has |

|                            |   |  |
|----------------------------|---|--|
|                            |   | to be used during the hash value computation.  |
|                            | TruncationIsAllowed   | This parameter states whether a truncation of the result is allowed or not.<br>TRUE: Truncation is allowed.<br>FALSE: Truncation is not allowed.   |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | resultLengthPtr   | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by resultPtr.<br>On returning from this function the actual length of the computed value shall be stored. |
| <b>Parameters (out):</b>   | resultPtr   | Holds a pointer to the memory location which will hold the result of the hash value computation. If the result does not fit into the given buffer, and truncation is allowed, the result shall be truncated.   |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result, and truncation was not allowed.  |
| <b>Description:</b>        | <p>This function shall be used to finish the hash service of the CAL module.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer.</p> <p>The hash computation is done by the underlying primitive.</p> |  |

⌋()

## [CAL0661]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small and truncation is allowed, the result of the computation shall be truncated to the size of the provided buffer, and CAL\_E\_OK shall be returned. If the provided buffer is too small, and truncation is not allowed, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_HashFinish.

### 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 Cal\_MacGenerateStart

[CAL0108] ⌈

|                            |  |   |
|----------------------------|--|---|
| <b>Service name:</b>       | Cal_MacGenerateStart   |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_MacGenerateStart(     Cal_ConfigIdType cfgId,     Cal_MacGenerateCtxBufType contextBuffer,     const Cal_SymKeyType* keyPtr )</pre>  |   |
| <b>Service ID[hex]:</b>    | 0x06   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the MAC computation. |
|                            | keyPtr   | Holds a pointer to the key necessary for the MAC generation.  |
| <b>Parameters (inout):</b> | None   |   |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
|                            |  |   |
| <b>Description:</b>        | <p>This function shall be used to initialize the MAC generate service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |   |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_MacGenerateStart.

### 8.3.3.2 Cal\_MacGenerateUpdate

[CAL0114] ⌈

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_MacGenerateUpdate   |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_MacGenerateUpdate(     Cal_ConfigIdType cfgId,     Cal_MacGenerateCtxBufType contextBuffer,     const uint8* dataPtr,     uint32 dataLength )</pre> |   |
| <b>Service ID[hex]:</b>    | 0x07  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the MAC computation. |
|                            | dataPtr   | Holds a pointer to the data for which a MAC shall be computed.  |
|                            | dataLength  | Contains the number of bytes for which the MAC shall be computed.                                     |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                   |

|                          |  |  |
|--------------------------|--|--|
| <b>Parameters (out):</b> | None   |  |
| <b>Return value:</b>     | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed |
| <b>Description:</b>      | <p>This function shall be used to feed the MAC generate service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The MAC computation is done by the underlying primitive.</p> |  |

()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_MacGenerateUpdate.

### 8.3.3.3 Cal\_MacGenerateFinish

[CAL0121] ↑

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_MacGenerateFinish  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_MacGenerateFinish(     Cal_ConfigIdType cfgId,     Cal_MacGenerateCtxBufType contextBuffer,     uint8* resultPtr,     uint32* resultLengthPtr,     boolean TruncationIsAllowed )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x08   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the MAC computation.  |
|                            | TruncationIsAllowed  | This parameter states whether a truncation of the result is allowed or not.<br>TRUE: Truncation is allowed.<br>FALSE: Truncation is not allowed.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | resultLengthPtr  | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by resultPtr.<br>On returning from this function the actual length of the computed MAC shall be stored. |
| <b>Parameters (out):</b>   | resultPtr  | Holds a pointer to the memory location which will hold the result of the MAC generation. If the result does not fit into the given buffer, and truncation is allowed, the result shall be truncated.   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result, and truncation was not allowed.  |
| <b>Description:</b>        | <p>This function shall be used to finish the MAC generation service.</p> <p>If the service state given by the context buffer is "idle", the function has to return</p>   |  |

|  |   |
|--|---|
|  | <p>with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The MAC computation is done by the underlying primitive.</p> |
|--|---|

⌋()

#### [CAL0662]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small and truncation is allowed, the result of the computation shall be truncated to the size of the provided buffer, and CAL\_E\_OK shall be returned. If the provided buffer is too small, and truncation is not allowed, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_MacGenerateFinish.

#### 8.3.3.4 Cal\_MacVerifyStart

##### [CAL0128] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_MacVerifyStart   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_MacVerifyStart(     Cal_ConfigIdType cfgId,     Cal_MacVerifyCtxBufType contextBuffer,     const Cal_SymKeyType* keyPtr )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x09   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the MAC verification. |
|                            | keyPtr   | Holds a pointer to the key necessary for the MAC verification.   |
| <b>Parameters (inout):</b> | None   |  |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                    |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to initialize the MAC verify service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_MacVerifyStart.

### 8.3.3.5 Cal\_MacVerifyUpdate

[CAL0134] ↑

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_MacVerifyUpdate   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_MacVerifyUpdate(     Cal_ConfigIdType cfgId,     Cal_MacVerifyCtxBufType contextBuffer,     const uint8* dataPtr,     uint32 dataLength )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x0A  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the MAC verification. |
|                            | dataPtr   | Holds a pointer to the data for which a MAC shall be verified.   |
|                            | dataLength  | Contains the number of bytes for which the MAC shall be verified.                                      |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                    |
| <b>Parameters (out):</b>   | None  |  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to feed the MAC verification service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The MAC computation is done by the underlying primitive. The MAC computation is done by the underlying primitive.</p> |  |

↓()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_MacVerifyUpdate.

### 8.3.3.6 Cal\_MacVerifyFinish

[CAL0141] ↑

|                         |  |  |
|-------------------------|--|--|
| <b>Service name:</b>    | Cal_MacVerifyFinish  |  |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_MacVerifyFinish(     Cal_ConfigIdType cfgId,     Cal_MacVerifyCtxBufType contextBuffer,     const uint8* MacPtr,     uint32 MacLength,     Cal_VerifyResultType* resultPtr )</pre> |  |
| <b>Service ID[hex]:</b> | 0x0B   |  |
| <b>Sync/Async:</b>      | Synchronous  |  |
| <b>Reentrancy:</b>      | Reentrant  |  |
| <b>Parameters (in):</b> | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the MAC verification. |

|                            |  |  |
|----------------------------|--|--|
|                            | MacPtr   | Holds a pointer to the memory location which will hold the MAC to verify.                  |
|                            | MacLength  | Holds the length of the MAC to be verified.  |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.        |
| <b>Parameters (out):</b>   | resultPtr  | Holds a pointer to the memory location which will hold the result of the MAC verification. |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed                               |
| <b>Description:</b>        | <p>This function shall be used to finish the MAC verification service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The MAC computation is done by the underlying primitive. The MAC computation is done by the underlying primitive.</p> |  |

l()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_MacVerifyFinish.

### 8.3.4 Random interface

The random interface provides generation of random numbers. The randomness of pseudo random number generators can be increased by an appropriate selection of the seed.

#### 8.3.4.1 Cal\_RandomSeedStart

[CAL0149] ⌈

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_RandomSeedStart   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_RandomSeedStart(     Cal_ConfigIdType cfgId,     Cal_RandomCtxBufType contextBuffer )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x0C  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the seeding of the random number generator. |
| <b>Parameters (inout):</b> | None  |  |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | This function shall be used to initialize the random seed service of the CAL  |  |



|  |  |
|--|--|
|  | <p>module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |
|--|--|

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_RandomSeedStart.

### 8.3.4.2 Cal\_RandomSeedUpdate

[CAL0156] 「

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_RandomSeedUpdate   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_RandomSeedUpdate(     Cal_ConfigIdType cfgId,     Cal_RandomCtxBufType contextBuffer,     const uint8* seedPtr,     uint32 seedLength )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x0D   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the seeding of the random number generator. |
|                            | seedPtr  | Holds a pointer to the seed for the random number generator.   |
|                            | seedLength   | Contains the length of the seed in bytes.  |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to feed a seed to the random number generator.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The seeding of the random number generator is done by the underlying primitive.</p> |  |

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_RandomSeedUpdate.

### 8.3.4.3 Cal\_RandomSeedFinish

[CAL0163] 「

|                      |                      |
|----------------------|----------------------|
| <b>Service name:</b> | Cal_RandomSeedFinish |
|----------------------|----------------------|



|                            |  |  |
|----------------------------|--|--|
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_RandomSeedFinish(     Cal_ConfigIdType cfgId,     Cal_RandomCtxBufType contextBuffer )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x0E   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the seeding of the random number generator. |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored   |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to finish the random seed service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The seeding of the random number generator is done by the underlying primitive</p> |  |

()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_RandomSeedFinish.

#### 8.3.4.4 Cal\_RandomGenerate

[CAL0543] ↑

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_RandomGenerate  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_RandomGenerate(     Cal_ConfigIdType cfgId,     Cal_RandomCtxBufType contextBuffer,     uint8* resultPtr,     uint32 resultLength )</pre> |   |
| <b>Service ID[hex]:</b>    | 0x0F  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during random number generation   |
|                            | resultLength  | Holds the amount of random bytes which should be generated.   |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored. If a seed is needed, this must be the same context buffer that has been used for the call of the RandomSeed interfaces. |
| <b>Parameters (out):</b>   | resultPtr   | Holds a pointer to the memory location which will hold the result of the random number generation. The memory location must have at least the size "resultLength".  |

|                      |  |  |
|----------------------|--|--|
| <b>Return value:</b> | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_ENTROPY_EXHAUSTION: Request failed, entropy of random number generator is exhausted. |
| <b>Description:</b>  | This function shall be used to start the random number generation service of the CAL module.<br><br>The function shall call the function Cpl_<Primitive> of the primitive which is identified by the "cfgId" and return the value returned by that function. |  |

l()

The generation of a random number is based on the seed, which was previously set with the interfaces Cal\_RandomSeedStart, Cal\_RandomSeedUpdate, and Cal\_RandomSeedFinish. These interfaces follow the streaming approach. Thus it is possible to feed the seed e.g. from different sources.

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

The APIs of the Random service are designed for usage of pseudo random number generators (PRNGs). True random number generators (TRNGs) are not supported.

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_RandomGenerate.

### 8.3.5 Symmetrical block interface

A block cipher is a symmetric key cipher operating on fixed-length blocks, with an unvarying transformation. A block cipher encryption algorithm might take (for example) a 128-bit block of plaintext as input, and output a corresponding 128-bit block of ciphertext. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit block of ciphertext together with the secret key, and yields the original 128-bit block of plaintext.

#### 8.3.5.1 Cal\_SymBlockEncryptStart

[CAL0168] ↑

|                         |   |   |
|-------------------------|---|---|
| <b>Service name:</b>    | Cal_SymBlockEncryptStart  |   |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_SymBlockEncryptStart(     Cal_ConfigIdType cfgId,     Cal_SymBlockEncryptCtxBufType contextBuffer,     const Cal_SymKeyType* keyPtr )</pre> |   |
| <b>Service ID[hex]:</b> | 0x10  |   |
| <b>Sync/Async:</b>      | Synchronous   |   |
| <b>Reentrancy:</b>      | Reentrant   |   |
| <b>Parameters (in):</b> | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the symmetrical block encryption |

|                            |   |  |
|----------------------------|---|--|
|                            |   | computation.   |
|                            | keyPtr  | Holds a pointer to the key which has to be used during the symmetrical block encryption computation. |
| <b>Parameters (inout):</b> | None  |  |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to initialize the symmetrical block encrypt service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymBlockEncryptStart.

### 8.3.5.2 Cal\_SymBlockEncryptUpdate

[CAL0173] 「

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_SymBlockEncryptUpdate  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymBlockEncryptUpdate(     Cal_ConfigIdType cfgId,     Cal_SymBlockEncryptCtxBufType contextBuffer,     const uint8* plainTextPtr,     uint32 plainTextLength,     uint8* cipherTextPtr,     uint32* cipherTextLengthPtr )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x11   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the symmetrical block encryption computation.   |
|                            | plainTextPtr   | Holds a pointer to the plain text that shall be encrypted.   |
|                            | plainTextLength  | Contains the length of the plain text in bytes.  |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | cipherTextLengthPtr  | <p>Holds a pointer to a memory location in which the length information is stored.</p> <p>On calling this function this parameter shall contain the size of the buffer provided by cipherTextPtr.</p> <p>On returning from this function the amount of data that has been encrypted shall be stored.</p> |
| <b>Parameters (out):</b>   | cipherTextPtr  | Holds a pointer to the memory location which will hold the encrypted text.   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |

|                     |   |
|---------------------|---|
| <b>Description:</b> | <p>This function shall be used to feed the symmetrical block encryption service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The encryption process is done by the underlying primitive.</p> |
|---------------------|---|

」()

### [CAL0663]

「 The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. 」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymBlockEncryptUpdate.

### 8.3.5.3 Cal\_SymBlockEncryptFinish

#### [CAL0180] 「

|                            |  |   |
|----------------------------|--|---|
| <b>Service name:</b>       | Cal_SymBlockEncryptFinish  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymBlockEncryptFinish(     Cal_ConfigIdType cfgId,     Cal_SymBlockEncryptCtxBufType contextBuffer )</pre>   |   |
| <b>Service ID[hex]:</b>    | 0x12   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the symmetrical block encryption computation.            |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.   |
| <b>Parameters (out):</b>   | None   |   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result. |
| <b>Description:</b>        | <p>This function shall be used to finish the symmetrical block encryption service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The encryption process is done by the underlying primitive.</p> |   |

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymBlockEncryptFinish.

#### 8.3.5.4 Cal\_SymBlockDecryptStart

[CAL0187] ⌈

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_SymBlockDecryptStart  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymBlockDecryptStart(     Cal_ConfigIdType cfgId,     Cal_SymBlockDecryptCtxBufType contextBuffer,     const Cal_SymKeyType* keyPtr )</pre>   |   |
| <b>Service ID[hex]:</b>    | 0x13  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the constant CAL module configuration which has to be used during the symmetrical block decryption computation. |
|                            | keyPtr  | Holds a pointer to the key which has to be used during the symmetrical block decryption computation.                                    |
| <b>Parameters (inout):</b> | None  |   |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to initialize the symmetrical block decrypt service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |   |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymBlockDecryptStart.

#### 8.3.5.5 Cal\_SymBlockDecryptUpdate

[CAL0192] ⌈

|                         |  |  |
|-------------------------|--|--|
| <b>Service name:</b>    | Cal_SymBlockDecryptUpdate  |  |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_SymBlockDecryptUpdate(     Cal_ConfigIdType cfgId,     Cal_SymBlockDecryptCtxBufType contextBuffer,     const uint8* cipherTextPtr,     uint32 cipherTextLength,     uint8* plainTextPtr,     uint32* plainTextLengthPtr )</pre> |  |
| <b>Service ID[hex]:</b> | 0x14   |  |
| <b>Sync/Async:</b>      | Synchronous  |  |

|                            |  |  |
|----------------------------|--|--|
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the constant CAL module configuration which has to be used during the symmetrical block decryption computation.  |
|                            | cipherTextPtr  | Holds a pointer to the constant cipher text that shall be decrypted.   |
|                            | cipherTextLength   | Contains the length of the cipher text in bytes.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | plainTextLengthPtr   | Holds a pointer to a memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by plainTextPtr.<br>On returning from this function the amount of data that has been decrypted shall be stored. |
| <b>Parameters (out):</b>   | plainTextPtr   | Holds a pointer to the memory location which will hold the decrypted text.   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to feed the symmetrical block decryption service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function. The decryption process is done by the underlying primitive.</p> |  |

⌋()

## [CAL0664]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned.

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymBlockDecryptUpdate. ⌋()

### 8.3.5.6 Cal\_SymBlockDecryptFinish

## [CAL0199] ⌈

|                            |  |   |
|----------------------------|--|---|
| <b>Service name:</b>       | Cal_SymBlockDecryptFinish  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymBlockDecryptFinish(     Cal_ConfigIdType cfgId,     Cal_SymBlockDecryptCtxBufType contextBuffer )</pre> |   |
| <b>Service ID[hex]:</b>    | 0x15   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the constant CAL module configuration which has to be used during the symmetrical block decryption computation. |
|                            | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.   |
| <b>Parameters (inout):</b> |  |   |

|                          |  |   |
|--------------------------|--|---|
| <b>Parameters (out):</b> | None   |   |
| <b>Return value:</b>     | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result. |
| <b>Description:</b>      | <p>This function shall be used to finish the symmetrical block decryption service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The decryption process is done by the underlying primitive.</p> |   |

()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymBlockDecryptFinish.

### 8.3.6 Symmetrical interface

Symmetric-key algorithms are algorithms that use identical cryptographic keys for both decryption and encryption. The keys, in practice, represent a shared secret between two or more parties.

#### 8.3.6.1 Cal\_SymEncryptStart

[CAL0206] ↑

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_SymEncryptStart  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymEncryptStart(     Cal_ConfigIdType cfgId,     Cal_SymEncryptCtxBufType contextBuffer,     const Cal_SymKeyType* keyPtr,     const uint8* InitVectorPtr,     uint32 InitVectorLength )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x16   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the symmetrical encryption computation. |
|                            | keyPtr   | Holds a pointer to the key which has to be used during the symmetrical encryption computation.                           |
|                            | InitVectorPtr  | Holds a pointer to the initialisation vector which has to be used during the symmetrical encryption computation.         |
|                            | InitVectorLength   | Holds the length of the initialisation vector which has to be used during the symmetrical encryption computation.        |
| <b>Parameters (inout):</b> | None   |  |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                                      |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful   |



|                     |   |
|---------------------|---|
|                     | CAL_E_NOT_OK: Request failed  |
| <b>Description:</b> | <p>This function shall be used to initialize the symmetrical encrypt service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |

()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymEncryptStart.

### 8.3.6.2 Cal\_SymEncryptUpdate

[CAL0212] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_SymEncryptUpdate   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymEncryptUpdate(     Cal_ConfigIdType cfgId,     Cal_SymEncryptCtxBufType contextBuffer,     const uint8* plainTextPtr,     uint32 plainTextLength,     uint8* cipherTextPtr,     uint32* cipherTextLengthPtr )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x17   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the symmetrical encryption computation.   |
|                            | plainTextPtr   | Holds a pointer to the plain text that shall be encrypted.   |
|                            | plainTextLength  | Contains the length of the plain text in bytes.  |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | cipherTextLengthPtr  | <p>Holds a pointer to a memory location in which the length information is stored.</p> <p>On calling this function this parameter shall contain the size of the buffer provided by cipherTextPtr.</p> <p>On returning from this function the amount of data that has been encrypted shall be stored.</p> |
| <b>Parameters (out):</b>   | cipherTextPtr  | Holds a pointer to the memory location which will hold the encrypted text.   |
| <b>Return value:</b>       | Cal_ReturnType   | <p>CAL_E_OK: Request successful</p> <p>CAL_E_NOT_OK: Request failed</p> <p>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.</p>   |
| <b>Description:</b>        | <p>This function shall be used to feed the symmetrical encryption service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that</p> |  |



|  |  |
|--|--|
|  | function.<br>The encryption process is done by the underlying primitive. |
|--|--|

」()

#### [CAL0665]

「 The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. 」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymEncryptUpdate.

### 8.3.6.3 Cal\_SymEncryptFinish

#### [CAL0221]「

|                          |  |   |
|--------------------------|--|---|
| <b>Service name:</b>     | Cal_SymEncryptFinish   |   |
| <b>Syntax:</b>           | <pre>Cal_ReturnType Cal_SymEncryptFinish(     Cal_ConfigIdType cfgId,     Cal_SymEncryptCtxBufType contextBuffer,     uint8* cipherTextPtr,     uint32* cipherTextLengthPtr )</pre>  |   |
| <b>Service ID[hex]:</b>  | 0x18   |   |
| <b>Sync/Async:</b>       | Synchronous  |   |
| <b>Reentrancy:</b>       | Reentrant  |   |
| <b>Parameters (in):</b>  | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the symmetrical encryption computation.  |
|                          | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.   |
|                          | cipherTextLengthPtr  | Holds a pointer to a memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by cipherTextPtr.<br>On returning from this function the amount of data that has been encrypted shall be stored. |
| <b>Parameters (out):</b> | cipherTextPtr  | Holds a pointer to the memory location which will hold the encrypted text.  |
| <b>Return value:</b>     | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.   |
| <b>Description:</b>      | <p>This function shall be used to finish the symmetrical encryption service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The encryption process is done by the underlying primitive.</p> |   |

」()

#### [CAL0666]

「 The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. 」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymEncryptFinish.

#### 8.3.6.4 Cal\_SymDecryptStart

##### [CAL0228] 「

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_SymDecryptStart   |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymDecryptStart(     Cal_ConfigIdType cfgId,     Cal_SymDecryptCtxBufType contextBuffer,     const Cal_SymKeyType* keyPtr,     const uint8* InitVectorPtr,     uint32 InitVectorLength )</pre>  |   |
| <b>Service ID[hex]:</b>    | 0x19  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the constant CAL module configuration which has to be used during the symmetrical decryption computation. |
|                            | keyPtr  | Holds a pointer to the key which has to be used during the symmetrical decryption computation.                                    |
|                            | InitVectorPtr   | Holds a pointer to the initialisation vector which has to be used during the symmetrical decryption computation.                  |
|                            | InitVectorLength  | Holds the length of the initialisation vector which has to be used during the symmetrical decryption computation.                 |
| <b>Parameters (inout):</b> | None  |   |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to initialize the symmetrical decrypt service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |   |

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymDecryptStart.

### 8.3.6.5 Cal\_SymDecryptUpdate

[CAL0234] ⌈

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_SymDecryptUpdate  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymDecryptUpdate(     Cal_ConfigIdType cfgId,     Cal_SymDecryptCtxBufType contextBuffer,     const uint8* cipherTextPtr,     uint32 cipherTextLength,     uint8* plainTextPtr,     uint32* plainTextLengthPtr )</pre>  |   |
| <b>Service ID[hex]:</b>    | 0x1A  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the symmetrical decryption computation.  |
|                            | cipherTextPtr   | Holds a pointer to the constant cipher text that shall be decrypted.  |
|                            | cipherTextLength  | Contains the length of the cipher text in bytes.  |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
|                            | plainTextLengthPtr  | <p>Holds a pointer to a memory location in which the length information is stored.</p> <p>On calling this function this parameter shall contain the size of the buffer provided by plainTextPtr.</p> <p>On returning from this function the amount of data that has been decrypted shall be stored.</p> |
| <b>Parameters (out):</b>   | plainTextPtr  | Holds a pointer to the memory location which will hold the decrypted text.  |
| <b>Return value:</b>       | Cal_ReturnType  | <p>CAL_E_OK: Request successful</p> <p>CAL_E_NOT_OK: Request failed</p> <p>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.</p>  |
| <b>Description:</b>        | <p>This function shall be used to feed the symmetrical decryption service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The decryption process is done by the underlying primitive.</p> |   |

⌋()

[CAL0667]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymDecryptUpdate.

### 8.3.6.6 Cal\_SymDecryptFinish

[CAL0243] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_SymDecryptFinish   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymDecryptFinish(     Cal_ConfigIdType cfgId,     Cal_SymDecryptCtxBufType contextBuffer,     uint8* plainTextPtr,     uint32* plainTextLengthPtr )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x1B   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the symmetrical decryption computation.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | plainTextLengthPtr   | Holds a pointer to a memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by plainTextPtr.<br>On returning from this function the amount of data that has been decrypted shall be stored. |
| <b>Parameters (out):</b>   | plainTextPtr   | Holds a pointer to the memory location which will hold the decrypted text.   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.  |
| <b>Description:</b>        | <p>This function shall be used to finish the symmetrical decryption service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The decryption process is done by the underlying primitive.</p> |  |

⌋()

[CAL0668]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymDecryptFinish.

### 8.3.7 Asymmetrical interface

Asymmetric-key algorithms are algorithms that use pairs of cryptographic keys (public and private keys) for decryption and encryption. The private key, in practice, represent a secret while the public key can be made publically available.

#### 8.3.7.1 Cal\_AsymEncryptStart

[CAL0250] ⌈

|                            |  |   |
|----------------------------|--|---|
| <b>Service name:</b>       | Cal_AsymEncryptStart   |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymEncryptStart(     Cal_ConfigIdType cfgId,     Cal_AsymEncryptCtxBufType contextBuffer,     const Cal_AsymPublicKeyType* keyPtr )</pre>   |   |
| <b>Service ID[hex]:</b>    | 0x1C   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the asymmetrical encryption computation. |
|                            | keyPtr   | Holds a pointer to the key which has to be used during the asymmetrical encryption computation.                           |
| <b>Parameters (inout):</b> | None   |   |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                                       |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to initialize the asymmetrical encrypt service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |   |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymEncryptStart.

#### 8.3.7.2 Cal\_AsymEncryptUpdate

[CAL0256] ⌈

|                      |  |  |
|----------------------|--|--|
| <b>Service name:</b> | Cal_AsymEncryptUpdate  |  |
| <b>Syntax:</b>       | <pre>Cal_ReturnType Cal_AsymEncryptUpdate(     Cal_ConfigIdType cfgId,     Cal_AsymEncryptCtxBufType contextBuffer,     const uint8* plainTextPtr,     uint32 plainTextLength,     uint8* cipherTextPtr,     uint32* cipherTextLengthPtr )</pre> |  |

|                            |  |   |
|----------------------------|--|---|
| <b>Service ID[hex]:</b>    | 0x1D   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the asymmetrical encryption computation.   |
|                            | plainTextPtr   | Holds a pointer to the memory location which will hold the encrypted text.  |
|                            | plainTextLength  | Contains the length of the plain text in bytes.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.   |
|                            | cipherTextLengthPtr  | Holds a pointer to a memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by cipherTextPtr.<br>On returning from this function the amount of data that has been encrypted shall be stored. |
| <b>Parameters (out):</b>   | cipherTextPtr  | Holds a pointer to the memory location which will hold the encrypted text.  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.   |
| <b>Description:</b>        | <p>This function shall be used to feed the asymmetrical encryption service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The encryption process is done by the underlying primitive.</p> |   |

⌋()

## [CAL0669]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymEncryptUpdate.

### 8.3.7.3 Cal\_AsymEncryptFinish

#### [CAL0265] ⌈

|                         |   |  |
|-------------------------|---|--|
| <b>Service name:</b>    | Cal_AsymEncryptFinish   |  |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_AsymEncryptFinish(     Cal_ConfigIdType cfgId,     Cal_AsymEncryptCtxBufType contextBuffer,     uint8* cipherTextPtr,     uint32* cipherTextLengthPtr )</pre> |  |
| <b>Service ID[hex]:</b> | 0x1E  |  |

|                            |   |   |
|----------------------------|---|---|
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the asymmetrical encryption computation.   |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
|                            | cipherTextLengthPtr   | Holds a pointer to a memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by cipherTextPtr.<br>On returning from this function the amount of data that has been encrypted shall be stored. |
| <b>Parameters (out):</b>   | cipherTextPtr   | Holds a pointer to the memory location which will hold the encrypted text.  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.   |
| <b>Description:</b>        | <p>This function shall be used to finish the asymmetrical encryption service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The encryption process is done by the underlying primitive.</p> |   |

⌋()

#### [CAL0670]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymEncryptFinish.

#### 8.3.7.4 Cal\_AsymDecryptStart

##### [CAL0272] ⌈

|                         |   |  |
|-------------------------|---|--|
| <b>Service name:</b>    | Cal_AsymDecryptStart  |  |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_AsymDecryptStart(     Cal_ConfigIdType cfgId,     Cal_AsymDecryptCtxBufType contextBuffer,     const Cal_AsymPrivateKeyType* keyPtr )</pre> |  |
| <b>Service ID[hex]:</b> | 0x1F  |  |
| <b>Sync/Async:</b>      | Synchronous   |  |
| <b>Reentrancy:</b>      | Reentrant   |  |
| <b>Parameters (in):</b> | cfgId   | Holds the identifier of the CAL module configuration which has |



|                            |  |   |
|----------------------------|--|---|
|                            |  | to be used during the asymmetrical decryption computation.                                      |
|                            | keyPtr   | Holds a pointer to the key which has to be used during the asymmetrical encryption computation. |
| <b>Parameters (inout):</b> | None   |   |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.             |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed                                    |
| <b>Description:</b>        | <p>This function shall be used to initialize the asymmetrical decrypt service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |   |

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymDecryptStart.

### 8.3.7.5 Cal\_AsymDecryptUpdate

[CAL0278] 「

|                            |  |   |
|----------------------------|--|---|
| <b>Service name:</b>       | Cal_AsymDecryptUpdate  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymDecryptUpdate(     Cal_ConfigIdType cfgId,     Cal_AsymDecryptCtxBufType contextBuffer,     const uint8* cipherTextPtr,     uint32 cipherTextLength,     uint8* plainTextPtr,     uint32* plainTextLengthPtr )</pre> |   |
| <b>Service ID[hex]:</b>    | 0x20   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the asymmetrical decryption computation.   |
|                            | cipherTextPtr  | Holds a pointer to the encrypted data.  |
|                            | cipherTextLength   | Contains the length of the encrypted data in bytes.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.   |
|                            | plainTextLengthPtr   | <p>Holds a pointer to a memory location in which the length information is stored.</p> <p>On calling this function this parameter shall contain the size of the buffer provided by plainTextPtr.</p> <p>On returning from this function the amount of data that has been decrypted shall be stored.</p> |
| <b>Parameters (out):</b>   | plainTextPtr   | Holds a pointer to the memory location which will hold the decrypted text.  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.   |



|                     |  |
|---------------------|--|
| <b>Description:</b> | <p>This function shall be used to feed the asymmetrical decryption service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The decryption process is done by the underlying primitive.</p> |
|---------------------|--|

」()

### [CAL0671]

「 The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. 」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymDecryptUpdate.

### 8.3.7.6 Cal\_AsymDecryptFinish

#### [CAL0287] 「

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_AsymDecryptFinish  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymDecryptFinish(     Cal_ConfigIdType cfgId,     Cal_AsymDecryptCtxBufType contextBuffer,     uint8* plainTextPtr,     uint32* plainTextLengthPtr )</pre>                  |  |
| <b>Service ID[hex]:</b>    | 0x21   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the asymmetrical computation.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | plainTextLengthPtr   | Holds a pointer to a memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by plainTextPtr.<br>On returning from this function the amount of data that has been decrypted shall be stored. |
| <b>Parameters (out):</b>   | plainTextPtr   | Holds a pointer to the memory location which will hold the decrypted text.   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.  |
| <b>Description:</b>        | <p>This function shall be used to finish the asymmetrical decryption service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> |  |

|  |   |
|--|---|
|  | Otherwise, this function shall call the function Cpl_<Primitive>Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_<Primitive>Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The decryption process is done by the underlying primitive. |
|--|---|

」()

#### [CAL0672]

「 The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. 」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymDecryptFinish.

### 8.3.8 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.

#### 8.3.8.1 Cal\_SignatureGenerateStart

##### [CAL0294]

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_SignatureGenerateStart  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SignatureGenerateStart(     Cal_ConfigIdType cfgId,     Cal_SignatureGenerateCtxBufType contextBuffer,     const Cal_AsymPrivateKeyType* keyPtr )</pre>               |  |
| <b>Service ID[hex]:</b>    | 0x22  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the signature generation. |
|                            | keyPtr  | Holds a pointer to the key necessary for the signature generation.   |
| <b>Parameters (inout):</b> | None  |  |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                        |
|                            |   |  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
|                            |   |  |
| <b>Description:</b>        | <p>This function shall be used to initialize the signature generate service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the</p> |  |

|  |  |
|--|--|
|  | function Cpl_<Primitive>Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_<Primitive>Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer. |
|--|--|

l()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SignatureGenerateStart.

### 8.3.8.2 Cal\_SignatureGenerateUpdate

[CAL0300] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_SignatureGenerateUpdate  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SignatureGenerateUpdate(     Cal_ConfigIdType cfgId,     Cal_SignatureGenerateCtxBufType contextBuffer,     const uint8* dataPtr,     uint32 dataLength )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x23   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the signature generation. |
|                            | dataPtr  | Holds a pointer to the data that shall be signed.  |
|                            | dataLength   | Contains the length of the data to be signed.  |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                        |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to feed the signature generation service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The signature computation is done by the underlying primitive.</p> |  |

l()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SignatureGenerateUpdate.

### 8.3.8.3 Cal\_SignatureGenerateFinish

[CAL0307] ⌈

|                      |   |  |
|----------------------|---|--|
| <b>Service name:</b> | Cal_SignatureGenerateFinish   |  |
| <b>Syntax:</b>       | <pre>Cal_ReturnType Cal_SignatureGenerateFinish(     Cal_ConfigIdType cfgId,     Cal_SignatureGenerateCtxBufType contextBuffer,</pre> |  |

|                            |   |   |
|----------------------------|---|---|
|                            | <pre>uint8* resultPtr, uint32* resultLengthPtr )</pre>  |   |
| <b>Service ID[hex]:</b>    | 0x24  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the signature generation.  |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
|                            | resultLengthPtr   | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by resultPtr.<br>On returning from this function the actual length of the computed signature shall be stored |
| <b>Parameters (out):</b>   | resultPtr   | Holds a pointer to the memory location which will hold the result of the signature generation.  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result  |
| <b>Description:</b>        | <p>This function shall be used to finish the signature generation service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The signature computation is done by the underlying primitive.</p> |   |

⌋()

### [CAL0673]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SignatureGenerateFinish.

### 8.3.8.4 Cal\_SignatureVerifyStart

#### [CAL0314] ⌈

|                         |  |  |
|-------------------------|--|--|
| <b>Service name:</b>    | Cal_SignatureVerifyStart   |  |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_SignatureVerifyStart(     Cal_ConfigIdType cfgId,     Cal_SignatureVerifyCtxBufType contextBuffer,     const Cal_AsymPublicKeyType* keyPtr )</pre> |  |
| <b>Service ID[hex]:</b> | 0x25   |  |
| <b>Sync/Async:</b>      | Synchronous  |  |
| <b>Reentrancy:</b>      | Reentrant  |  |

|                            |  |  |
|----------------------------|--|--|
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the signature computation/verification. |
|                            | keyPtr   | Holds a pointer to the key necessary for the signature verification.   |
| <b>Parameters (inout):</b> | None   |  |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                                      |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to initialize the signature verify service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SignatureVerifyStart.

### 8.3.8.5 Cal\_SignatureVerifyUpdate

[CAL0320] 「

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_SignatureVerifyUpdate   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SignatureVerifyUpdate(     Cal_ConfigIdType cfgId,     Cal_SignatureVerifyCtxBufType contextBuffer,     const uint8* dataPtr,     uint32 dataLength )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x26  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the signature computation/verification. |
|                            | dataPtr   | Holds a pointer to the signature which shall be verified.  |
|                            | dataLength  | Contains the length of the signature to verify in bytes.   |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                                      |
| <b>Parameters (out):</b>   | None  |  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to feed the signature verification service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function. The signature computation is done by the underlying primitive.</p> |  |

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SignatureVerifyUpdate.

### 8.3.8.6 Cal\_SignatureVerifyFinish

[CAL0327] 「

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_SignatureVerifyFinish   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SignatureVerifyFinish(     Cal_ConfigIdType cfgId,     Cal_SignatureVerifyCtxBufType contextBuffer,     const uint8* signaturePtr,     uint32 signatureLength,     Cal_VerifyResultType* resultPtr )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x27  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the signature computation/verification. |
|                            | signaturePtr  | Holds a pointer to the memory location which holds the signature to be verified.   |
|                            | signatureLength   | Holds the length of the Signature to be verified.  |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                                      |
| <b>Parameters (out):</b>   | resultPtr   | Holds a pointer to the memory location which will hold the result of the signature verification.                         |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to finish the signature verification service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The signature computation is done by the underlying primitive.</p> |  |

」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SignatureVerifyFinish.

### 8.3.9 Checksum interface

The goal of checksum algorithms is to detect accidental modification such as corruption to stored data or errors in a communication channel. They are not designed to detect intentional corruption by a malicious agent. Indeed, many

checksum algorithms can be easily inverted, in the sense that one can easily modify the data so as to preserve its checksum.

### 8.3.9.1 Cal\_ChecksumStart

[CAL0335] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_ChecksumStart  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_ChecksumStart(     Cal_ConfigIdType cfgId,     Cal_ChecksumCtxBufType contextBuffer )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x28   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the checksum computation. |
| <b>Parameters (inout):</b> | None   |  |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                        |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to initialize the checksum service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_ChecksumStart.

### 8.3.9.2 Cal\_ChecksumUpdate

[CAL0341] ⌈

|                         |   |  |
|-------------------------|---|--|
| <b>Service name:</b>    | Cal_ChecksumUpdate  |  |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_ChecksumUpdate(     Cal_ConfigIdType cfgId,     Cal_ChecksumCtxBufType contextBuffer,     const uint8* dataPtr,     uint32 dataLength )</pre> |  |
| <b>Service ID[hex]:</b> | 0x29  |  |
| <b>Sync/Async:</b>      | Synchronous   |  |
| <b>Reentrancy:</b>      | Reentrant   |  |
| <b>Parameters (in):</b> | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the checksum computation. |
|                         | dataPtr   | Holds a pointer to the data for which the checksum shall be calculated.                                    |



|                            |   |   |
|----------------------------|---|---|
|                            | dataLength  | Contains the length of the input data in bytes.                                     |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored. |
| <b>Parameters (out):</b>   | None  |   |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed                        |
| <b>Description:</b>        | <p>This function shall be used to feed the checksum service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The checksum computation is done by the underlying primitive.</p> |   |

()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_ChecksumUpdate.

### 8.3.9.3 Cal\_ChecksumFinish

[CAL0348] ↑

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_ChecksumFinish   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_ChecksumFinish(     Cal_ConfigIdType cfgId,     Cal_ChecksumCtxBufType contextBuffer,     uint8* resultPtr,     uint32* resultLengthPtr,     boolean TruncationIsAllowed )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x2A   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the checksum computation.   |
|                            | TruncationIsAllowed  | This parameter states whether a truncation of the result is allowed or not.<br>TRUE: Truncation is allowed.<br>FALSE: Truncation is not allowed.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | resultLengthPtr  | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by resultPtr.<br>On returning from this function the actual length of the computed checksum shall be stored |
| <b>Parameters (out):</b>   | resultPtr  | Holds a pointer to the memory location which will hold the result of the checksum calculation. If the result does not fit into the given buffer, the result shall be truncated.  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |



|                     |  |   |
|---------------------|--|---|
|                     |  | CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result, and truncation was not allowed. |
| <b>Description:</b> | <p>This function shall be used to finish the checksum service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The checksum computation is done by the underlying primitive.</p> |   |

⌋()

#### [CAL0674]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small and truncation is allowed, the result of the computation shall be truncated to the size of the provided buffer, and CAL\_E\_OK shall be returned. If the provided buffer is too small, and truncation is not allowed, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_ChecksumFinish.

### 8.3.10 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.

#### 8.3.10.1 Cal\_KeyDeriveStart

##### [CAL0355] ⌈

|                         |  |  |
|-------------------------|--|--|
| <b>Service name:</b>    | Cal_KeyDeriveStart   |  |
| <b>Syntax:</b>          | <pre>Cal_ReturnType Cal_KeyDeriveStart(     Cal_ConfigIdType cfgId,     Cal_KeyDeriveCtxBufType contextBuffer,     uint32 keyLength,     uint32 iterations )</pre> |  |
| <b>Service ID[hex]:</b> | 0x2B   |  |
| <b>Sync/Async:</b>      | Synchronous  |  |
| <b>Reentrancy:</b>      | Reentrant  |  |
| <b>Parameters (in):</b> | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key derivation. |
|                         | keyLength  | Holds the length of the key to be derived by the underlying key derivation primitive.                |
|                         | iterations   | Holds the number of iterations to be performed by the underlying key derivation primitive.           |
| <b>Parameters</b>       | None   |  |

|                          |  |   |
|--------------------------|--|---|
| <b>(inout):</b>          |  |   |
| <b>Parameters (out):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored. |
| <b>Return value:</b>     | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed                        |
| <b>Description:</b>      | <p>This function shall be used to initialize the key derivation service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |   |

()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_KeyDeriveStart.

### 8.3.10.2 Cal\_KeyDeriveUpdate

[CAL0362] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_KeyDeriveUpdate  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_KeyDeriveUpdate(     Cal_ConfigIdType cfgId,     Cal_KeyDeriveCtxBufType contextBuffer,     const uint8* passwordPtr,     uint32 passwordLength,     const uint8* saltPtr,     uint32 saltLength )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x2C   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key derivation. |
|                            | passwordPtr  | Holds a pointer to the password, i.e. the original key, from which to derive a new key.              |
|                            | passwordLength   | Holds the length of the password in bytes.   |
|                            | saltPtr  | Holds a pointer to the cryptographic salt, i.e. a random number, for the underlying primitive.       |
|                            | saltLength   | Holds the length of the salt in bytes.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                  |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to feed the key derivation service with the input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that</p> |  |

|  |  |
|--|--|
|  | function.<br>The key derivation computation is done by the underlying primitive. |
|--|--|

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_KeyDeriveUpdate.

### 8.3.10.3 Cal\_KeyDeriveFinish

[CAL0371] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_KeyDeriveFinish  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_KeyDeriveFinish(     Cal_ConfigIdType cfgId,     Cal_KeyDeriveCtxBufType contextBuffer,     Cal_SymKeyType* keyPtr )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x2D   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key derivation. |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                  |
| <b>Parameters (out):</b>   | keyPtr   | Holds a pointer to the memory location which will hold the result of the key derivation.             |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to finish the key generation service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The key derivation computation is done by the underlying primitive.</p> |  |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_KeyDeriveFinish.

### 8.3.11 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.

### 8.3.11.1 Cal\_KeyExchangeCalcPubVal

[CAL0377] 「

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_KeyExchangeCalcPubVal  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_KeyExchangeCalcPubVal(     Cal_ConfigIdType cfgId,     const Cal_KeyExchangeBaseType* basePtr,     const Cal_KeyExchangePrivateType* privateValuePtr,     uint8* publicValuePtr,     uint32* publicValueLengthPtr )</pre>            |  |
| <b>Service ID[hex]:</b>    | 0x2E   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration that has to be used during the key exchange.  |
|                            | basePtr  | Holds a pointer to the base information known to both users of the key exchange protocol.  |
|                            | privateValuePtr  | Holds a pointer to the private information known only to the current user of the key exchange protocol.  |
| <b>Parameters (inout):</b> | publicValueLengthPtr   | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by publicValuePtr.<br>On returning from this function the actual length of the calculated public value shall be stored. |
| <b>Parameters (out):</b>   | publicValuePtr   | Holds a pointer to the memory location which will hold the public value of the key exchange protocol.  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result.  |
| <b>Description:</b>        | This function shall be used to start the public value calculation service of the CAL module.<br><br>The function shall call the function Cpl_<Primitive> of the primitive which is identified by the "cfgId" and return the value returned by that function. |  |

」()

[CAL0675]

「 The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small, CAL\_E\_SMALL\_BUFFER shall be returned. 」()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_KeyExchangeCalcPubVal.

### 8.3.11.2 Cal\_KeyExchangeCalcSecretStart

[CAL0396] 「

|                      |                                |
|----------------------|--------------------------------|
| <b>Service name:</b> | Cal_KeyExchangeCalcSecretStart |
|----------------------|--------------------------------|

|                            |  |   |
|----------------------------|--|---|
| <b>Syntax:</b>             | <pre> Cal_ReturnType Cal_KeyExchangeCalcSecretStart(     Cal_ConfigIdType cfgId,     Cal_KeyExchangeCalcSecretCtxBufType contextBuffer,     const Cal_KeyExchangeBaseType* basePtr,     const Cal_KeyExchangePrivateType* privateValuePtr ) </pre>   |   |
| <b>Service ID[hex]:</b>    | 0x2F   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration that has to be used during the key exchange.       |
|                            | basePtr  | Holds a pointer to the base information known to both users of the key exchange protocol.               |
|                            | privateValuePtr  | Holds a pointer to the private information known only to the current user of the key exchange protocol. |
| <b>Parameters (inout):</b> | None   |   |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                     |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to initialize the key exchange service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |   |

()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_KeyExchangeCalcSecretStart.

### 8.3.11.3 Cal\_KeyExchangeCalcSecretUpdate

[CAL0404] ↑

|                         |   |   |
|-------------------------|---|---|
| <b>Service name:</b>    | Cal_KeyExchangeCalcSecretUpdate   |   |
| <b>Syntax:</b>          | <pre> Cal_ReturnType Cal_KeyExchangeCalcSecretUpdate(     Cal_ConfigIdType cfgId,     Cal_KeyExchangeCalcSecretCtxBufType contextBuffer,     const uint8* partnerPublicValuePtr,     uint32 partnerPublicValueLength ) </pre> |   |
| <b>Service ID[hex]:</b> | 0x30  |   |
| <b>Sync/Async:</b>      | Synchronous   |   |
| <b>Reentrancy:</b>      | Reentrant   |   |
| <b>Parameters (in):</b> | cfgId   | Holds the identifier of the CAL module configuration that has to be used during the key exchange. |
|                         | partnerPublicValuePtr   | Holds a pointer to the data representing the public value of the key exchange partner.            |
|                         | partnerPublicValueLength  | Contains the length of the part of the partner value in   |

|                            |  |   |
|----------------------------|--|---|
|                            |  | bytes.  |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored. |
| <b>Parameters (out):</b>   | None   |   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed                        |
| <b>Description:</b>        | <p>This function shall be used to feed the key exchange service with the public value coming from the partner of the key exchange protocol.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The calculation of the shared secret is done by the underlying primitive.</p> |   |

()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_KeyExchangeCalcSecretUpdate.

#### 8.3.11.4 Cal\_KeyExchangeCalcSecretFinish

[CAL0411]†

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_KeyExchangeCalcSecretFinish  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_KeyExchangeCalcSecretFinish(     Cal_ConfigIdType cfgId,     Cal_KeyExchangeCalcSecretCtxBufType contextBuffer,     uint8* sharedSecretPtr,     uint32* sharedSecretLengthPtr,     boolean TruncationIsAllowed )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x31   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration that has to be used during the key exchange.  |
|                            | TruncationIsAllowed  | This parameter states whether a truncation of the result is allowed or not.<br>TRUE: Truncation is allowed.<br>FALSE: Truncation is not allowed.   |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.  |
|                            | sharedSecretLengthPtr  | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by sharedSecretPtr.<br>On returning from this function the actual length of the computed value shall be stored. |
| <b>Parameters (out):</b>   | sharedSecretPtr  | Holds a pointer to the memory location which will hold the result of the key exchange. If the result does not fit into the given buffer, and truncation is allowed, the result shall be truncated.   |

|                      |  |   |
|----------------------|--|---|
| <b>Return value:</b> | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed<br>CAL_E_SMALL_BUFFER: The provided buffer is too small to store the result, and truncation was not allowed. |
| <b>Description:</b>  | <p>This function shall be used to finish the key exchange service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The calculation of the shared secret is done by the underlying primitive.</p> |   |

⌋()

### [CAL0676]

⌈ The CAL shall check if the provided buffer is large enough to hold the result of the computation. If the provided buffer is too small and truncation is allowed, the result of the computation shall be truncated to the size of the provided buffer, and CAL\_E\_OK shall be returned. If the provided buffer is too small, and truncation is not allowed, CAL\_E\_SMALL\_BUFFER shall be returned. ⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_KeyExchangeCalcSecretFinish.

## 8.3.12 Symmetrical key extract interface

Symmetrical key extract interface is used to extract a symmetrical key structure from certain data sources.

Note that this interface may be used for key transport purposes. In this case, any necessary auxiliary information (e.g., wrapping key, shared information, randomness) will have to be encoded unambiguously into the data provided in the dataPtr buffer.

### 8.3.12.1 Cal\_SymKeyExtractStart

#### [CAL0418] ⌈

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_SymKeyExtractStart  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymKeyExtractStart(     Cal_ConfigIdType cfgId,     Cal_SymKeyExtractCtxBufType contextBuffer )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x32  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key extraction. |
| <b>Parameters (inout):</b> | None  |  |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this   |



|                      |  |  |
|----------------------|--|--|
|                      |  | service can be stored.                                       |
| <b>Return value:</b> | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed |
| <b>Description:</b>  | <p>This function shall be used to initialize the symmetrical key extraction service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymKeyExtractStart.

### 8.3.12.2 Cal\_SymKeyExtractUpdate

[CAL0425] ⌈

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_SymKeyExtractUpdate   |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymKeyExtractUpdate(     Cal_ConfigIdType cfgId,     Cal_SymKeyExtractCtxBufType contextBuffer,     const uint8* dataPtr,     uint32 dataLength )</pre>   |   |
| <b>Service ID[hex]:</b>    | 0x33  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key extraction.  |
|                            | dataPtr   | Holds a pointer to the data which contains the key in a format which cannot be used directly by the CAL. From this data the key will be extracted in a CAL-conforming format. |
|                            | dataLength  | Holds the length of the data in bytes.  |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
| <b>Parameters (out):</b>   | None  |   |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to feed the symmetrical key extraction service with input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function. The calculation of the extraction algorithm is done by the underlying primitive.</p> |   |

⌋()



Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymKeyExtractUpdate.

### 8.3.12.3 Cal\_SymKeyExtractFinish

[CAL0432] ⌈

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_SymKeyExtractFinish   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymKeyExtractFinish(     Cal_ConfigIdType cfgId,     Cal_SymKeyExtractCtxBufType contextBuffer,     Cal_SymKeyType* keyPtr )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x34  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key extraction. |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                  |
| <b>Parameters (out):</b>   | keyPtr  | Holds a pointer to a structure where the result (i.e. the symmetrical key) is stored in.             |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to finish the symmetrical key extraction service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The calculation of the extraction algorithm is done by the underlying primitive.</p> |  |

⌋()

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_SymKeyExtractFinish.

### 8.3.13 Symmetrical key wrapping interface

Symmetrical key wrapping interface is used to export a symmetrical key structure, e.g. to be used on a different device. To be able to use symmetric and asymmetric wrapping keys, two different interfaces are standardised.

#### 8.3.13.1 Cal\_SymKeyWrapSymStart

[CAL0744] ⌈

|                      |  |  |
|----------------------|--|--|
| <b>Service name:</b> | Cal_SymKeyWrapSymStart                 |  |
| <b>Syntax:</b>       | Cal_ReturnType Cal_SymKeyWrapSymStart( |  |

|                            |   |  |
|----------------------------|---|--|
|                            | <pre> Cal_ConfigIdType cfgId, Cal_SymKeyWrapSymCtxBufType contextBuffer, const Cal_SymKeyType* keyPtr, const Cal_SymKeyType* wrappingKeyPtr ) </pre>  |  |
| <b>Service ID[hex]:</b>    | 0x3c  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key wrapping. |
|                            | keyPtr  | Holds a pointer to the symmetric key to be wrapped.  |
|                            | wrappingKeyPtr  | Holds a pointer to the key used for wrapping.  |
| <b>Parameters (inout):</b> | None  |  |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                |
|                            | Cal_ReturnType  | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed                                       |
| <b>Description:</b>        | <p>This interface shall be used to initialize the symmetrical key wrapping service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable. \_()

### 8.3.13.2 Cal\_SymKeyWrapSymUpdate

[CAL0745] ↑

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_SymKeyWrapSymUpdate   |   |
| <b>Syntax:</b>             | <pre> Cal_ReturnType Cal_SymKeyWrapSymUpdate(     Cal_ConfigIdType cfgId,     Cal_SymKeyWrapSymCtxBufType contextBuffer,     uint8* dataPtr,     uint32* dataLengthPtr ) </pre> |   |
| <b>Service ID[hex]:</b>    | 0x3d  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key wrapping.  |
|                            | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
| <b>Parameters (inout):</b> | dataLengthPtr   | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by dataPtr.<br>When the request has finished, the actual length of the computed value shall be stored. |

|                          |  |   |
|--------------------------|--|---|
| <b>Parameters (out):</b> | dataPtr  | Holds a pointer to the memory location which will hold the first chunk of the result of the key wrapping. If the result does not fit into the given buffer, the caller shall call the service again, until *dataLengthPtr is equal to zero, indicating that the complete result has been retrieved. |
| <b>Return value:</b>     | Cal_ReturnType   | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed  |
| <b>Description:</b>      | <p>This interface shall be used to retrieve the result of the key wrapping operation from the symmetrical key wrapping service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function. The calculation of the extraction algorithm is done by the underlying primitive.</p> |   |

Regarding error detection, the requirements CAL0064, CAL0488 and CAL0489 are applicable. ⌋()

### 8.3.13.3 Cal\_SymKeyWrapSymFinish

[CAL0746] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_SymKeyWrapSymFinish  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymKeyWrapSymFinish(     Cal_ConfigIdType cfgId,     Cal_SymKeyWrapSymCtxBufType contextBuffer )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x3e   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key wrapping. |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed                                       |
| <b>Description:</b>        | <p>This interface shall be used to finish the symmetrical key wrapping service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The calculation of the extraction algorithm is done by the underlying primitive.</p> |  |

Regarding error detection, the requirements CAL0064, CAL0488 and CAL0489 are applicable. ⌋()

## 8.3.13.4 Cal\_SymKeyWrapAsymStart

[CAL0747] ⌈

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_SymKeyWrapAsymStart   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymKeyWrapAsymStart(     Cal_ConfigIdType cfgId,     Cal_SymKeyWrapAsymCtxBufType contextBuffer,     const Cal_SymKeyType* keyPtr,     const Cal_AsymPublicKeyType* wrappingKeyPtr )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x3f  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CSM module configuration which has to be used during the key wrapping. |
|                            | keyPtr  | Holds a pointer to the symmetric key to be wrapped.  |
|                            | wrappingKeyPtr  | Holds a pointer to the public key used for wrapping.   |
| <b>Parameters (inout):</b> | None  |  |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed                                       |
| <b>Description:</b>        | <p>This interface shall be used to initialize the symmetrical key wrapping service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable. ⌋()

## 8.3.13.5 Cal\_SymKeyWrapAsymUpdate

[CAL0748] ⌈

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_SymKeyWrapAsymUpdate  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymKeyWrapAsymUpdate(     Cal_ConfigIdType cfgId,     Cal_SymKeyWrapAsymCtxBufType contextBuffer,     uint8* dataPtr,     uint32* dataLengthPtr )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x40  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key wrapping. |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                |

|                          |  |   |
|--------------------------|--|---|
|                          | dataLengthPtr  | Holds a pointer to the memory location in which the length information is stored.   |
| <b>Parameters (out):</b> | dataPtr  | Holds a pointer to the memory location which will hold the first chunk of the result of the key wrapping. If the result does not fit into the given buffer, the caller shall call the service again, until *dataLengthPtr is equal to zero, indicating that the complete result has been retrieved. |
| <b>Return value:</b>     | Cal_ReturnType   | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed<br>CAL_E_BUSY: request failed, service is still busy   |
| <b>Description:</b>      | <p>This interface shall be used to retrieve the result of the key wrapping operation from the symmetrical key wrapping service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function. The calculation of the extraction algorithm is done by the underlying primitive.</p> |   |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable. ⌋()

### 8.3.13.6 Cal\_SymKeyWrapAsymFinish

[CAL0749] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_SymKeyWrapAsymFinish   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_SymKeyWrapAsymFinish(     Cal_ConfigIdType cfgId,     Cal_SymKeyWrapAsymCtxBufType contextBuffer )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x41   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key wrapping. |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed                                       |
| <b>Description:</b>        | <p>This interface shall be used to finish the symmetrical key wrapping service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The calculation of the extraction algorithm is done by the underlying primitive.</p> |  |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable. 」()

### 8.3.14 Asymmetrical key extract interfaces

Asymmetrical key extract interface is used to extract an asymmetrical key structure (e.g. public and private key pair) from certain data sources.

Note that this interface may be used for key transport purposes. In this case, any necessary auxiliary information (e.g., wrapping key, shared information, randomness) will have to be encoded unambiguously into the data provided in the dataPtr buffer.

#### 8.3.14.1 Cal\_AsymPublicKeyExtractStart

[CAL0436]「

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_AsymPublicKeyExtractStart  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPublicKeyExtractStart(     Cal_ConfigIdType cfgId,     Cal_AsymPublicKeyExtractCtxBufType contextBuffer )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x35   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key extraction. |
| <b>Parameters (inout):</b> | None   |  |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to initialize the asymmetrical public key extraction service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymPublicKeyExtractStart. 」()

#### 8.3.14.2 Cal\_AsymPublicKeyExtractUpdate

[CAL0443]「

|                      |   |  |
|----------------------|---|--|
| <b>Service name:</b> | Cal_AsymPublicKeyExtractUpdate  |  |
| <b>Syntax:</b>       | <pre>Cal_ReturnType Cal_AsymPublicKeyExtractUpdate(     Cal_ConfigIdType cfgId,     Cal_AsymPublicKeyExtractCtxBufType contextBuffer,     const uint8* dataPtr,     uint32 dataLength )</pre> |  |

|                            |  |   |
|----------------------------|--|---|
|                            | )  |   |
| <b>Service ID[hex]:</b>    | 0x36   |   |
| <b>Sync/Async:</b>         | Synchronous  |   |
| <b>Reentrancy:</b>         | Reentrant  |   |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key extraction.  |
|                            | dataPtr  | Holds a pointer to the data which contains the key in a format which cannot be used directly by the CAL. From this data the key will be extracted in a CAL-conforming format. |
|                            | dataLength   | Holds the length of the data in bytes.  |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.   |
| <b>Parameters (out):</b>   | None   |   |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to feed the asymmetrical public key extraction service with input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The calculation of the extraction algorithm is done by the underlying primitive.</p> |   |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymPublicKeyExtractUpdate. »()

### 8.3.14.3 Cal\_AsymPublicKeyExtractFinish

[CAL0450]†

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_AsymPublicKeyExtractFinish  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPublicKeyExtractFinish(     Cal_ConfigIdType cfgId,     Cal_AsymPublicKeyExtractCtxBufType contextBuffer,     Cal_AsymPublicKeyType* keyPtr )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x37  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key extraction. |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                  |
| <b>Parameters (out):</b>   | keyPtr  | Holds a pointer to a structure where the result (i.e. the symmetrical key) is stored in.             |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | This function shall be used to finish the asymmetrical public key extraction service.   |  |



|  |  |
|--|--|
|  | <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The calculation of the extraction algorithm is done by the underlying primitive.</p> |
|--|--|

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymPublicKeyExtractFinish. \_j()

#### 8.3.14.4 Cal\_AsymPrivateKeyExtractStart

[CAL0680] ⌈

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_AsymPrivateKeyExtractStart  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPrivateKeyExtractStart(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyExtractCtxBufType contextBuffer )</pre>   |  |
| <b>Service ID[hex]:</b>    | 0x38  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key extraction. |
| <b>Parameters (inout):</b> | None  |  |
| <b>Parameters (out):</b>   | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | <p>This function shall be used to initialize the asymmetrical private key extraction service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymPrivateKeyExtractStart. \_j()

#### 8.3.14.5 Cal\_AsymPrivateKeyExtractUpdate

[CAL0682] ⌈

|                      |   |  |
|----------------------|---|--|
| <b>Service name:</b> | Cal_AsymPrivateKeyExtractUpdate   |  |
| <b>Syntax:</b>       | <pre>Cal_ReturnType Cal_AsymPrivateKeyExtractUpdate(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyExtractCtxBufType contextBuffer,</pre> |  |



|                            |   |   |
|----------------------------|---|---|
|                            | <pre>const uint8* dataPtr, uint32 dataLength )</pre>  |   |
| <b>Service ID[hex]:</b>    | 0x39  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key extraction.  |
|                            | dataPtr   | Holds a pointer to the data which contains the key in a format which cannot be used directly by the CAL. From this data the key will be extracted in a CAL-conforming format. |
|                            | dataLength  | Holds the length of the data in bytes.  |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
| <b>Parameters (out):</b>   | None  |   |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed  |
| <b>Description:</b>        | <p>This function shall be used to feed the asymmetrical private key extraction service with input data.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function.</p> <p>The calculation of the extraction algorithm is done by the underlying primitive.</p> |   |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymPrivateKeyExtractUpdate. ]()

### 8.3.14.6 Cal\_AsymPrivateKeyExtractFinish

[CAL0684] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_AsymPrivateKeyExtractFinish  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPrivateKeyExtractFinish(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyExtractCtxBufType contextBuffer,     Cal_AsymPrivateKeyType* keyPtr )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x3A   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key extraction. |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                  |
| <b>Parameters (out):</b>   | keyPtr   | Holds a pointer to a structure where the result (i.e. the symmetrical key) is stored in.             |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: Request successful<br>CAL_E_NOT_OK: Request failed   |
| <b>Description:</b>        | This function shall be used to finish the asymmetrical private key extraction  |  |

|  |  |
|--|--|
|  | <p>service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The calculation of the extraction algorithm is done by the underlying primitive.</p> |
|--|--|

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable to the function Cal\_AsymPrivateKeyExtractFinish. \_()

### 8.3.15 Asymmetrical key wrapping interface

Asymmetrical key wrapping interface is used to export a (asymmetric) private key structure, e.g. to be used on a different device. To be able to use symmetric and asymmetric wrapping keys, two different interfaces are standardised.

#### 8.3.15.1 Cal\_AsymPrivateKeyWrapSymStart

[CAL0750] ⌈

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_AsymPrivateKeyWrapSymStart   |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPrivateKeyWrapSymStart(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyWrapSymCtxBufType contextBuffer,     const Cal_AsymPrivateKeyType* keyPtr,     const Cal_SymKeyType* wrappingKeyPtr )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x42   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CAL module configuration which has to be used during the key wrapping. |
|                            | keyPtr   | Holds a pointer to the private key to be wrapped.  |
|                            | wrappingKeyPtr   | Holds a pointer to the key used for wrapping.  |
| <b>Parameters (inout):</b> | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed                                       |
|                            |  |  |
| <b>Description:</b>        | <p>This interface shall be used to initialize the asymmetrical key wrapping service of the CAL module.</p> <p>The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_&lt;Primitive&gt;Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_&lt;Primitive&gt;Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer.</p> |  |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable.  $\lrcorner()$

### 8.3.15.2 Cal\_AsymPrivateKeyWrapSymUpdate

[CAL0751]  $\lrcorner$

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_AsymPrivateKeyWrapSymUpdate   |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPrivateKeyWrapSymUpdate(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyWrapSymCtxBufType contextBuffer,     uint8* dataPtr,     uint32* dataLengthPtr )</pre>   |   |
| <b>Service ID[hex]:</b>    | 0x43  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key wrapping.  |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
|                            | dataLengthPtr   | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by dataPtr.  |
| <b>Parameters (out):</b>   | dataPtr   | Holds a pointer to the memory location which will hold the first chunk of the result of the key wrapping. If the result does not fit into the given buffer, the caller shall call the service again, until *dataLengthPtr is equal to zero, indicating that the complete result has been retrieved. |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed  |
| <b>Description:</b>        | <p>This interface shall be used to retrieve the result of the key wrapping operation from the asymmetrical key wrapping service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function. The calculation of the extraction algorithm is done by the underlying primitive.</p> |   |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable.  $\lrcorner()$

### 8.3.15.3 Cal\_AsymPrivateKeyWrapSymFinish

[CAL0752]  $\lrcorner$

|                      |                                 |
|----------------------|---------------------------------|
| <b>Service name:</b> | Cal_AsymPrivateKeyWrapSymFinish |
|----------------------|---------------------------------|

|                            |   |  |
|----------------------------|---|--|
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPrivateKeyWrapSymFinish(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyWrapSymCtxBufType contextBuffer )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x44  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key wrapping. |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                |
| <b>Parameters (out):</b>   | None  |  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed                                       |
| <b>Description:</b>        | <p>This interface shall be used to finish the asymmetrical key wrapping service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The calculation of the extraction algorithm is done by the underlying primitive.</p> |  |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable. )()

#### 8.3.15.4 Cal\_AsymPrivateKeyWrapAsymStart

[CAL0753] ↑

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cal_AsymPrivateKeyWrapAsymStart  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPrivateKeyWrapAsymStart(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyWrapAsymCtxBufType contextBuffer,     const Cal_AsymPrivateKeyType* keyPtr,     const Cal_AsymPublicKeyType* wrappingKeyPtr )</pre> |  |
| <b>Service ID[hex]:</b>    | 0x45   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | cfgId  | Holds the identifier of the CSM module configuration which has to be used during the key wrapping. |
|                            | keyPtr   | Holds a pointer to the private key to be wrapped.  |
|                            | wrappingKeyPtr   | Holds a pointer to the public key used for wrapping.   |
| <b>Parameters (inout):</b> | None   |  |
| <b>Parameters (out):</b>   | contextBuffer  | Holds the pointer to the buffer in which the context of this service can be stored.                |
| <b>Return value:</b>       | Cal_ReturnType   | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed                                       |
| <b>Description:</b>        | <p>This interface shall be used to initialize the asymmetrical key wrapping service of the CAL module.</p>   |  |

|  |  |
|--|--|
|  | The function shall initialize the context buffer given by "contextBuffer", call the function Cpl_<Primitive>Start of the primitive which is identified by the "cfgId" and return the value returned by that function. If Cpl_<Primitive>Start returned successfully, the function shall set the state of this service to "active", and store this state in the context buffer. |
|--|--|

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable. \_()

### 8.3.15.5 Cal\_AsymPrivateKeyWrapAsymUpdate

[CAL0754]†

|                            |   |   |
|----------------------------|---|---|
| <b>Service name:</b>       | Cal_AsymPrivateKeyWrapAsymUpdate  |   |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPrivateKeyWrapAsymUpdate(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyWrapAsymCtxBufType contextBuffer,     uint8* dataPtr,     uint32* dataLengthPtr )</pre>   |   |
| <b>Service ID[hex]:</b>    | 0x46  |   |
| <b>Sync/Async:</b>         | Synchronous   |   |
| <b>Reentrancy:</b>         | Reentrant   |   |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key wrapping.  |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.   |
|                            | dataLengthPtr   | Holds a pointer to the memory location in which the length information is stored.<br>On calling this function this parameter shall contain the size of the buffer provided by dataPtr.<br>When the request has finished, the actual length of the computed value shall be stored.                   |
| <b>Parameters (out):</b>   | dataPtr   | Holds a pointer to the memory location which will hold the first chunk of the result of the key wrapping. If the result does not fit into the given buffer, the caller shall call the service again, until *dataLengthPtr is equal to zero, indicating that the complete result has been retrieved. |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed<br>CAL_E_BUSY: request failed, service is still busy   |
| <b>Description:</b>        | <p>This interface shall be used to retrieve the result of the key wrapping operation from the asymmetrical key wrapping service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Update of the primitive which is identified by the "cfgId", and return the value returned by that function. The calculation of the extraction algorithm is done by the underlying primitive.</p> |   |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable. \_()

### 8.3.15.6 Cal\_AsymPrivateKeyWrapAsymFinish

[CAL0755]⌈

|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cal_AsymPrivateKeyWrapAsymFinish  |  |
| <b>Syntax:</b>             | <pre>Cal_ReturnType Cal_AsymPrivateKeyWrapAsymFinish(     Cal_ConfigIdType cfgId,     Cal_AsymPrivateKeyWrapAsymCtxBufType contextBuffer )</pre>  |  |
| <b>Service ID[hex]:</b>    | 0x47  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | cfgId   | Holds the identifier of the CAL module configuration which has to be used during the key wrapping. |
| <b>Parameters (inout):</b> | contextBuffer   | Holds the pointer to the buffer in which the context of this service can be stored.                |
| <b>Parameters (out):</b>   | None  |  |
| <b>Return value:</b>       | Cal_ReturnType  | CAL_E_OK: request successful<br>CAL_E_NOT_OK: request failed                                       |
| <b>Description:</b>        | <p>This interface shall be used to finish the asymmetrical key wrapping service.</p> <p>If the service state given by the context buffer is "idle", the function has to return with "CAL_E_NOT_OK".</p> <p>Otherwise, this function shall call the function Cpl_&lt;Primitive&gt;Finish of the primitive which is identified by the "cfgId", and return the value returned by that function. If Cpl_&lt;Primitive&gt;Finish returned successfully, the function shall set the state of this service to "idle", and store this state in the context buffer. The calculation of the extraction algorithm is done by the underlying primitive.</p> |  |

Regarding error detection, the requirements [CAL0064](#), [CAL0488](#) and [CAL0489](#) are applicable. ⌋()

## 8.4 Dependencies to cryptographic library API functions

### 8.4.1 Types for the Cryptographic Primitives

#### 8.4.1.1 Cpl\_<Primitive>ConfigType

[CAL0544]⌈

|                     |  |
|---------------------|--|
| <b>Name:</b>        | Cpl_<Primitive>_ConfigType   |
| <b>Type:</b>        | Structure  |
| <b>Range:</b>       | Implementation specific.   |
| <b>Description:</b> | Data structure which shall encompass all information needed to specify the information needed for the <Primitive> cryptographic primitive. |

⌋()

## 8.4.2 API functions of the cryptographic primitives

### [CAL0461]

「 For every API function of a cryptographic service, the corresponding cryptographic primitive shall contain a corresponding function. 」(BSW42600006)

### [CAL0505]

「 The implementation of the basic cryptographic routines shall be synchronous and reentrant. 」()

### 8.4.2.1 Cpl\_<Primitive>Start

#### [CAL0701] 「

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cpl_<Primitive>Start   |  |
| <b>Syntax:</b>             | Cal_ReturnType Cpl_<Primitive>Start(<br><type> <xxx><br>)  |  |
| <b>Service ID[hex]:</b>    | --   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | <xxx>  | The arguments <xxx> shall be identical to the arguments of the corresponding function Cal_<Service>Start(), with the exception of the argument cfgId. This argument is of type "Cal_ConfigIdType" in Cal_<Service>Start(). In Cpl_<Primitive>Start the argument cfgId shall be replaced by an argument cfgPtr of type "const void **". |
| <b>Parameters (inout):</b> | None   |  |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | The return values shall be identical to those of the corresponding function Cal_<Service>Start().  |
| <b>Description:</b>        | This function shall initialize the computation of the cryptographic primitive, so that the primitive is able to process input data.<br>Intermediate results, that are required for further processing of the service, shall be stored in the context buffer, which is given as an argument of this function. |  |

」()

The API "Cpl\_<Primitive>Start" has a parameter "cfgPtr" of type "const void \*\*". When calling this API, the parameter "cfgPtr" shall point to a constant variable of type "Cpl\_<Primitive>ConfigType", but shall be cast to "const void \*\*". Reason for this is to have a common definition of the parameter list of this API for all primitives of one service, because in the structure Cal\_<Service>ConfigType one element is a function pointer to this API.

### 8.4.2.2 Cpl\_<Primitive>Update

#### [CAL0702] 「



|                            |   |  |
|----------------------------|---|--|
| <b>Service name:</b>       | Cpl_<Primitive>Update   |  |
| <b>Syntax:</b>             | Cal_ReturnType Cpl_<Primitive>Update(<br><type> <xxx><br>)  |  |
| <b>Service ID[hex]:</b>    | --  |  |
| <b>Sync/Async:</b>         | Synchronous   |  |
| <b>Reentrancy:</b>         | Reentrant   |  |
| <b>Parameters (in):</b>    | <xxx>   | The arguments <xxx> shall be identical to the arguments of the corresponding function Cal_<Service>Update(), with the exception of the argument cfgld. This argument is of type "Cal_ConfigldType" in Cal_<Service>Update(). In Cpl_<Primitive>Update the argument cfgld shall be replaced by an argument cfgPtr of type "const void *". |
| <b>Parameters (inout):</b> | None  |  |
| <b>Parameters (out):</b>   | None  |  |
| <b>Return value:</b>       | Cal_ReturnType  | The return values shall be identical to those of the corresponding function Cal_<Service>Update().   |
| <b>Description:</b>        | This function shall process a chunk of the given input data with the algorithm of the cryptographic primitive.<br>Intermediate results, that are derived from previous processing steps of this service, have to be taken from the context buffer, which is given as an argument of this function.<br>Intermediate results, that are required for further processing of the service, shall be stored in the context buffer, which is given as an argument of this function. |  |

()

The API "Cpl\_<Primitive>Update" has a parameter "cfgPtr" of type "const void \*". When calling this API, the parameter "cfgPtr" shall point to a constant variable of type "Cpl\_<Primitive>ConfigType", but shall be cast to "const void \*". Reason for this is to have a common definition of the parameter list of this API for all primitives of one service, because in the structure Cal\_<Service>ConfigType one element is a function pointer to this API.

#### 8.4.2.3 Cpl\_<Primitive>Finish

[CAL0703] ↑

|                            |  |  |
|----------------------------|--|--|
| <b>Service name:</b>       | Cpl_<Primitive>Finish                                      |  |
| <b>Syntax:</b>             | Cal_ReturnType Cpl_<Primitive>Finish(<br><type> <xxx><br>) |  |
| <b>Service ID[hex]:</b>    | --   |  |
| <b>Sync/Async:</b>         | Synchronous  |  |
| <b>Reentrancy:</b>         | Reentrant  |  |
| <b>Parameters (in):</b>    | <xxx>  | The arguments <xxx> shall be identical to the arguments of the corresponding function Cal_<Service>Finish(), with the exception of the argument cfgld. This argument is of type "Cal_ConfigldType" in Cal_<Service>Finish(). In Cpl_<Primitive>Finish the argument cfgld shall be replaced by an argument cfgPtr of type "const void *". |
| <b>Parameters (inout):</b> | None   |  |
| <b>Parameters (out):</b>   | None   |  |
| <b>Return value:</b>       | Cal_ReturnType   | The return values shall be identical to those of the corresponding   |



|                     |  |
|---------------------|--|
|                     | function Cal_<Service>Finish().  |
| <b>Description:</b> | This function shall finish the computation of the cryptographic primitive and store the result into the memory location given.<br>Intermediate results, that are derived from previous processing steps of this service, have to be taken from the context buffer, which is given as an argument of this function. |

⌋()

The API "Cpl\_<Primitive>Finish" has a parameter "cfgPtr" of type "const void \*".  
When calling this API, the parameter "cfgPtr" shall point to a constant variable of type "Cpl\_<Primitive>ConfigType", but shall be cast to "const void \*".  
Reason for this is to have a common definition of the parameter list of this API for all primitives of one service, because in the structure Cal\_<Service>ConfigType one element is a function pointer to this API.

#### 8.4.2.4 Cpl\_<Primitive>

[CAL0704] ⌈

|                            |   |
|----------------------------|---|
| <b>Service name:</b>       | Cpl_<Primitive>   |
| <b>Syntax:</b>             | Cal_ReturnType Cpl_<Primitive>(<br><type> <xxx><br>)  |
| <b>Service ID[hex]:</b>    | --  |
| <b>Sync/Async:</b>         | Synchronous   |
| <b>Reentrancy:</b>         | Reentrant   |
| <b>Parameters (in):</b>    | <xxx><br>The arguments <xxx> shall be identical to the arguments of the corresponding function Cal_<Service>(), with the exception of the argument cfgld. This argument is of type "Cal_ConfigldType" in Cal_<Service>(). In Cpl_<Primitive> the argument cfgld shall be replaced by an argument cfgPtr of type "const void *". |
| <b>Parameters (inout):</b> | None  |
| <b>Parameters (out):</b>   | None  |
| <b>Return value:</b>       | Cal_ReturnType<br>The return values shall be identical to those of the corresponding function Cal_<Service>().  |
| <b>Description:</b>        | This function shall process the cryptographic primitive with the given input data and store the result in the memory location given.  |

⌋()

The API "Cpl\_<Primitive>" has a parameter "cfgPtr" of type "const void \*".  
When calling this API, the parameter "cfgPtr" shall point to a constant variable of type "Cpl\_<Primitive>ConfigType", but shall be cast to "const void \*".  
Reason for this is to have a common definition of the parameter list of this API for all primitives of one service, because in the structure Cal\_<Service>ConfigType one element is a function pointer to this API.

### 8.4.3 Configuration of the cryptographic primitives

For each cryptographic primitive, a cryptographic library module has to provide a configuration structure. This configuration structure shall be of type `Cpl_<Primitive>ConfigType`. For each configuration of a primitive, the cryptographic library module has to provide a constant variable of that type. To link a primitive configuration to a specific service configuration, the corresponding parameter `Cal<Service>InitConfiguration` of the service configuration has to be set to the C-language symbol of the primitive configuration.

Variants of CPL modules with different optimization objectives may exist. These Variants should be handled by separate modules. Those optimizations may include execution speed, platform specific optimizations, RAM size and/or code segment size etc. The most suitable variant for a given deployment should be used.

## 9 Sequence diagrams

Not applicable.

## 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 CAL.

Chapter 10.3 specifies published information of the module CAL.

The CAL library shall not have any configuration options that may affect the functional behaviour of the routines. I.e. for a given set of input parameters, the outputs shall be always the same. For example, the returned value in case of error shall not be configurable.

However, a library vendor is allowed to add specific configuration options concerning library implementation, e.g. for resources consumption optimization.

**Note:** When changing the configuration of a cryptographical service, the result of a routine may change even without changing the input parameters. This is no contradiction to BSW31400001, because in this case a different configuration can be considered as using a different input parameter.

### 10.1 How to read this chapter

In addition to this section, it is highly recommended to read the documents:

- AUTOSAR Layered Software Architecture [\[2\]](#)
- AUTOSAR ECU Configuration Specification [\[4\]](#)  
This document describes the AUTOSAR configuration methodology and the AUTOSAR configuration metamodel in detail.

The following is only a short survey of the topic and it will not replace the ECU Configuration Specification document.

#### 10.1.1 Configuration and configuration parameters

Configuration parameters define the variability of the generic part(s) of an implementation of a module. This means that only generic or configurable module implementation can be adapted to the environment (software/hardware) in use during system and/or ECU configuration.

The configuration of parameters can be achieved at different times during the software process: before compile time, before link time or after build time. In the following, the term “configuration class” (of a parameter) shall be used in order to refer to a specific configuration point in time.

### 10.1.2 Variants

Variants describe sets of configuration parameters. E.g., variant 1: only pre-compile time configuration parameters; variant 2: mix of pre-compile- and post build time-configuration parameters. In one variant a parameter can only be of one configuration class.

### 10.1.3 Containers

Containers structure the set of configuration parameters. This means:

- *all* configuration parameters are kept in containers.
- (sub-) containers can reference (sub-) containers. It is possible to assign a multiplicity to these references. The multiplicity then defines the possible number of instances of the contained parameters.

## 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.

### 10.2.1 Variants

Variant1: This variant allows only pre-compile time configuration parameters.

### 10.2.2 Cal

|                           |   |
|---------------------------|---|
| <b>Module Name</b>        | <i>Cal</i>  |
| <b>Module Description</b> | Configuration of the Cal (CryptoAbstractionLibrary) module. |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CalAsymDecrypt             | 0..1                | Container for incorporation of AsymDecrypt primitives.            |
| CalAsymEncrypt             | 0..1                | Container for incorporation of AsymEncrypt primitives.            |
| CalAsymPrivateKeyExtract   | 0..1                | Container for incorporation of AsymPrivateKeyExtract primitives.  |
| CalAsymPrivateKeyWrapAsym  | 0..1                | Container for incorporation of AsymPrivateKeyWrapAsym primitives. |
| CalAsymPrivateKeyWrapSym   | 0..1                | Container for incorporation of AsymPrivateKeyWrapSym primitives.  |
| CalAsymPublicKeyExtract    | 0..1                | Container for incorporation of AsymPublicKeyExtract primitives.   |
| CalChecksum                | 0..1                | Container for incorporation of Checksum primitives.               |
| CalGeneral                 | 1                   | Container for common configuration options.                       |
| CalHash                    | 0..1                | Container for incorporation of Hash primitives.                   |
| CalKeyDerive               | 0..1                | Container for incorporation of KeyDerive primitives.              |
| CalKeyExchangeCalcPubVal   | 0..1                | Container for incorporation of KeyExchangeCalcPubVal primitives.  |
| CalKeyExchangeCalcSecret   | 0..1                | Container for incorporation of KeyExchangeCalcSecret              |

|                      |      |   |
|----------------------|------|---|
|                      |      | primitives.   |
| CalMacGenerate       | 0..1 | Container for incorporation of MacGenerate primitives.      |
| CalMacVerify         | 0..1 | Container for incorporation of MacVerify primitives.        |
| CalRandomGenerate    | 0..1 | Container for incorporation of RandomGenerate primitives.   |
| CalRandomSeed        | 0..1 | Container for incorporation of RandomSeed primitives.       |
| CalSignatureGenerate | 0..1 | Container for incorporation of SignatureGenerate primitives |
| CalSignatureVerify   | 0..1 | Container for incorporation of SignatureVerify primitives.  |
| CalSymBlockDecrypt   | 0..1 | Container for incorporation of SymBlockDecrypt primitives.  |
| CalSymBlockEncrypt   | 0..1 | Container for incorporation of SymBlockEncrypt primitives.  |
| CalSymDecrypt        | 0..1 | Container for incorporation of SymDecrypt primitives        |
| CalSymEncrypt        | 0..1 | Container for incorporation of SymEncrypt primitives.       |
| CalSymKeyExtract     | 0..1 | Container for incorporation of SymKeyExtract primitives.    |
| CalSymKeyWrapAsym    | 0..1 | Container for incorporation of SymKeyWrapAsym primitives.   |
| CalSymKeyWrapSym     | 0..1 | Container for incorporation of SymKeyWrapSym primitives.    |

### 10.2.3 CalGeneral

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0554_Conf :</b>                       |
| <b>Container Name</b>           | CalGeneral                                  |
| <b>Description</b>              | Container for common configuration options. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0744_Conf :</b>  |    |              |
| <b>Name</b>               | CalMaxAlignScalarType  |    |              |
| <b>Description</b>        | The scalar type which has the maximum alignment restrictions on the given platform. This type can be e.g. uint8, uint16 or uint32. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

**No Included Containers**

### 10.2.4 CalHash

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0559_Conf :</b>                           |
| <b>Container Name</b>           | CalHash   |
| <b>Description</b>              | Container for incorporation of Hash primitives. |
| <b>Configuration Parameters</b> |   |

|                    |  |  |  |
|--------------------|--|--|--|
| <b>SWS Item</b>    | <b>CAL0745_Conf :</b>  |  |  |
| <b>Name</b>        | CalHashMaxCtxBufByteSize   |  |  |
| <b>Description</b> | The maximum, in bytes, of all context buffers used in all CPL primitives |  |  |

|                           |                                     |    |              |
|---------------------------|-------------------------------------|----|--------------|
|                           | which implement a hash computation. |    |              |
| <b>Multiplicity</b>       | 1                                   |    |              |
| <b>Type</b>               | EcucIntegerParamDef                 |    |              |
| <b>Range</b>              | 1 .. 4294967295                     |    |              |
| <b>Default value</b>      | --                                  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>             | X  | All Variants |
|                           | <b>Link time</b>                    | -- |              |
|                           | <b>Post-build time</b>              | -- |              |
| <b>Scope / Dependency</b> | scope: module                       |    |              |

| <b>Included Containers</b> |                     |                                      |
|----------------------------|---------------------|--------------------------------------|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>            |
| CalHashConfig              | 0..32               | Configurations for the Hash service. |

### 10.2.5 CalHashConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0560 Conf :</b>  |
| <b>Container Name</b>           | CalHashConfig  |
| <b>Description</b>              | Configurations for the Hash service. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0563_Conf :</b>  |    |              |
| <b>Name</b>               | CalHashInitConfiguration   |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0562_Conf :</b>                       |    |              |
| <b>Name</b>               | CalHashPrimitiveName                        |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

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

## 10.2.6 CalMacGenerate

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0635_Conf :</b>                                  |
| <b>Container Name</b>           | CalMacGenerate   |
| <b>Description</b>              | Container for incorporation of MacGenerate primitives. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0746_Conf :</b>  |    |              |
| <b>Name</b>               | CalMacGenerateMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a MAC generation. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0709_Conf :</b>  |    |              |
| <b>Name</b>               | CalMacGenerateMaxKeySize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a MAC generation. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                            |                     |   |
|----------------------------|---------------------|---|
| <b>Included Containers</b> |                     |   |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                   |
| CalMacGenerateConfig       | 0..32               | Configurations for the MacGenerate service. |

## 10.2.7 CalMacGenerateConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0564_Conf :</b>   |
| <b>Container Name</b>           | CalMacGenerateConfig  |
| <b>Description</b>              | Configurations for the MacGenerate service. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                    |  |
|--------------------|--|
| <b>SWS Item</b>    | <b>CAL0567_Conf :</b>  |
| <b>Name</b>        | CalMacGenerateInitConfiguration  |
| <b>Description</b> | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |



|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Multiplicity</b>       | 1                       |    |              |
| <b>Type</b>               | EcucStringParamDef      |    |              |
| <b>Default value</b>      | --                      |    |              |
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0566_Conf :</b>                       |    |              |
| <b>Name</b>               | CalMacGeneratePrimitiveName                 |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

No Included Containers

## 10.2.8 CalMacVerify

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0636_Conf :</b>                                |
| <b>Container Name</b>           | CalMacVerify   |
| <b>Description</b>              | Container for incorporation of MacVerify primitives. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0747_Conf :</b>  |    |              |
| <b>Name</b>               | CalMacVerifyMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a MAC verification. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                     |  |  |  |
|---------------------|--|--|--|
| <b>SWS Item</b>     | <b>CAL0710_Conf :</b>  |  |  |
| <b>Name</b>         | CalMacVerifyMaxKeySize   |  |  |
| <b>Description</b>  | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a MAC verification. |  |  |
| <b>Multiplicity</b> | 1  |  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Type</b>               | EcucIntegerParamDef     |    |              |
| <b>Range</b>              | 1 .. 4294967295         |    |              |
| <b>Default value</b>      | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                 |
| CalMacVerifyConfig         | 0..32               | Configurations for the MacVerify service. |

### 10.2.9 CalMacVerifyConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0568_Conf :</b>   |
| <b>Container Name</b>           | CalMacVerifyConfig  |
| <b>Description</b>              | Container for configuration of service MacVerify. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0571_Conf :</b>  |    |              |
| <b>Name</b>               | CalMacVerifyInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0570_Conf :</b>                       |    |              |
| <b>Name</b>               | CalMacVerifyPrimitiveName                   |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

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

### 10.2.10 CalRandomSeed

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0641_Conf :</b>                                 |
| <b>Container Name</b>           | CalRandomSeed   |
| <b>Description</b>              | Container for incorporation of RandomSeed primitives. |
| <b>Configuration Parameters</b> |   |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0748_Conf :</b>   |    |              |
| <b>Name</b>               | CalRandomMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement seeding or generating a random number. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucIntegerParamDef   |    |              |
| <b>Range</b>              | 1 .. 4294967295   |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>   | X  | All Variants |
|                           | <b>Link time</b>  | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module   |    |              |

|                            |                     |  |
|----------------------------|---------------------|--|
| <b>Included Containers</b> |                     |  |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                  |
| CalRandomSeedConfig        | 0..32               | Configurations for the RandomSeed service. |

### 10.2.11 CalRandomSeedConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0642_Conf :</b>  |
| <b>Container Name</b>           | CalRandomSeedConfig  |
| <b>Description</b>              | Container for configuration of service RandomSeed. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0645_Conf :</b>  |    |              |
| <b>Name</b>               | CalRandomSeedInitConfiguration   |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                     |   |
|---------------------|---|
| <b>SWS Item</b>     | <b>CAL0644_Conf :</b>                       |
| <b>Name</b>         | CalRandomSeedPrimitiveName                  |
| <b>Description</b>  | Name of the cryptographic primitive to use. |
| <b>Multiplicity</b> | 1   |
| <b>Type</b>         | EcucStringParamDef                          |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Default value</b>      | --                      |    |              |
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

**No Included Containers**

### 10.2.12 CalRandomGenerate

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0620_Conf :</b>                                     |
| <b>Container Name</b>           | CalRandomGenerate   |
| <b>Description</b>              | Container for incorporation of RandomGenerate primitives. |
| <b>Configuration Parameters</b> |   |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                       |
| CalRandomGenerateConfig    | 0..32               | Configurations for the RandomGenerate service . |

### 10.2.13 CalRandomGenerateConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0637_Conf :</b>  |
| <b>Container Name</b>           | CalRandomGenerateConfig  |
| <b>Description</b>              | Container for configuration of service RandomGenerate. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0640_Conf :</b>  |    |              |
| <b>Name</b>               | CalRandomGeneratelnitConfiguration   |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                    |   |
|--------------------|---|
| <b>SWS Item</b>    | <b>CAL0639_Conf :</b>                       |
| <b>Name</b>        | CalRandomGeneratePrimitiveName              |
| <b>Description</b> | Name of the cryptographic primitive to use. |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Multiplicity</b>       | 1                       |    |              |
| <b>Type</b>               | EcucStringParamDef      |    |              |
| <b>Default value</b>      | --                      |    |              |
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

#### No Included Containers

### 10.2.14 CalSymBlockEncrypt

|                                 |  |  |  |
|---------------------------------|--|--|--|
| <b>SWS Item</b>                 | <b>CAL0621_Conf :</b>                                      |  |  |
| <b>Container Name</b>           | CalSymBlockEncrypt   |  |  |
| <b>Description</b>              | Container for incorporation of SymBlockEncrypt primitives. |  |  |
| <b>Configuration Parameters</b> |  |  |  |

|                    |  |    |              |
|--------------------|--|----|--------------|
| SWS Item           | CAL0749_Conf :   |    |              |
| Name               | CalSymBlockEncryptMaxCtxBufByteSize  |    |              |
| Description        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a symmetrical block encryption. |    |              |
| Multiplicity       | 1  |    |              |
| Type               | EcucIntegerParamDef  |    |              |
| Range              | 1 .. 4294967295  |    |              |
| Default value      | --   |    |              |
| ConfigurationClass | Pre-compile time   | X  | All Variants |
|                    | Link time  | -- |              |
|                    | Post-build time  | -- |              |
| Scope / Dependency | scope: module  |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0711_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymBlockEncryptMaxKeySize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a symmetrical block encryption. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                            |                     |  |
|----------------------------|---------------------|--|
| <b>Included Containers</b> |                     |  |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                        |
| CalSymBlockEncryptConfig   | 0..32               | Configurations for the SymBlockEncrypt service . |

### 10.2.15 CalSymBlockEncryptConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0572_Conf :</b>   |
| <b>Container Name</b>           | CalSymBlockEncryptConfig  |
| <b>Description</b>              | Container for configuration of service SymBlockEncrypt. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0575_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymBlockEncryptInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0574_Conf :</b>                       |    |              |
| <b>Name</b>               | CalSymBlockEncryptPrimitiveName             |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

No Included Containers

### 10.2.16 CalSymBlockDecrypt

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0622_Conf :</b>                                      |
| <b>Container Name</b>           | CalSymBlockDecrypt   |
| <b>Description</b>              | Container for incorporation of SymBlockDecrypt primitives. |
| <b>Configuration Parameters</b> |  |

|                     |  |  |  |
|---------------------|--|--|--|
| <b>SWS Item</b>     | <b>CAL0750_Conf :</b>  |  |  |
| <b>Name</b>         | CalSymBlockDecryptMaxCtxBufByteSize  |  |  |
| <b>Description</b>  | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a symmetrical block decryption. |  |  |
| <b>Multiplicity</b> | 1  |  |  |
| <b>Type</b>         | EcucIntegerParamDef  |  |  |

|                           |                         |                |
|---------------------------|-------------------------|----------------|
| <b>Range</b>              | 1 .. 4294967295         |                |
| <b>Default value</b>      | --                      |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X All Variants |
|                           | <b>Link time</b>        | --             |
|                           | <b>Post-build time</b>  | --             |
| <b>Scope / Dependency</b> | scope: module           |                |

|                           |  |                |
|---------------------------|--|----------------|
| <b>SWS Item</b>           | <b>CAL0712_Conf :</b>  |                |
| <b>Name</b>               | CalSymBlockDecryptMaxKeySize   |                |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a symmetrical block decryption. |                |
| <b>Multiplicity</b>       | 1  |                |
| <b>Type</b>               | EcucIntegerParamDef  |                |
| <b>Range</b>              | 1 .. 4294967295  |                |
| <b>Default value</b>      | --   |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X All Variants |
|                           | <b>Link time</b>   | --             |
|                           | <b>Post-build time</b>   | --             |
| <b>Scope / Dependency</b> | scope: module  |                |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                       |
| CalSymBlockDecryptConfig   | 0..32               | Configurations for the SymBlockDecrypt service. |

### 10.2.17 CalSymBlockDecryptConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0576_Conf :</b>   |
| <b>Container Name</b>           | CalSymBlockDecryptConfig  |
| <b>Description</b>              | Container for configuration of service SymBlockDecrypt. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |                |
|---------------------------|--|----------------|
| <b>SWS Item</b>           | <b>CAL0579_Conf :</b>  |                |
| <b>Name</b>               | CalSymBlockDecryptInitConfiguration  |                |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |                |
| <b>Multiplicity</b>       | 1  |                |
| <b>Type</b>               | EcucStringParamDef   |                |
| <b>Default value</b>      | --   |                |
| <b>maxLength</b>          | --   |                |
| <b>minLength</b>          | --   |                |
| <b>regularExpression</b>  | --   |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X All Variants |
|                           | <b>Link time</b>   | --             |
|                           | <b>Post-build time</b>   | --             |
| <b>Scope / Dependency</b> | scope: module  |                |

|                     |   |  |
|---------------------|---|--|
| <b>SWS Item</b>     | <b>CAL0578_Conf :</b>                       |  |
| <b>Name</b>         | CalSymBlockDecryptPrimitiveName             |  |
| <b>Description</b>  | Name of the cryptographic primitive to use. |  |
| <b>Multiplicity</b> | 1   |  |
| <b>Type</b>         | EcucStringParamDef                          |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Default value</b>      | --                      |    |              |
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

#### No Included Containers

### 10.2.18 CalSymEncrypt

|                                 |   |  |  |
|---------------------------------|---|--|--|
| <b>SWS Item</b>                 | <b>CAL0623_Conf :</b>                                 |  |  |
| <b>Container Name</b>           | CalSymEncrypt   |  |  |
| <b>Description</b>              | Container for incorporation of SymEncrypt primitives. |  |  |
| <b>Configuration Parameters</b> |   |  |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0751_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymEncryptMaxCtxBufByteSize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a symmetrical encryption. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0713_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymEncryptMaxKeySize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a symmetrical encryption. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                            |                     |  |
|----------------------------|---------------------|--|
| <b>Included Containers</b> |                     |  |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                  |
| CalSymEncryptConfig        | 0..32               | Configurations for the SymEncrypt service. |



### 10.2.19 CalSymEncryptConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0580_Conf :</b>  |
| <b>Container Name</b>           | CalSymEncryptConfig  |
| <b>Description</b>              | Container for configuration of service SymEncrypt. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0583_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymBlockEncryptInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0582_Conf :</b>                       |    |              |
| <b>Name</b>               | CalSymEncryptPrimitiveName                  |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

**No Included Containers**

### 10.2.20 CalSymDecrypt

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0624_Conf :</b>                                |
| <b>Container Name</b>           | CalSymDecrypt  |
| <b>Description</b>              | Container for incorporation of SymDecrypt primitives |
| <b>Configuration Parameters</b> |  |

|                     |  |  |  |
|---------------------|--|--|--|
| <b>SWS Item</b>     | <b>CAL0752_Conf :</b>  |  |  |
| <b>Name</b>         | CalSymDecryptMaxCtxBufByteSize   |  |  |
| <b>Description</b>  | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a symmetrical decryption. |  |  |
| <b>Multiplicity</b> | 1  |  |  |
| <b>Type</b>         | EcucIntegerParamDef  |  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Range</b>              | 1 .. 4294967295         |    |              |
| <b>Default value</b>      | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0714_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymDecryptMaxKeySize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a symmetrical decryption. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                   |
| CalSymDecryptConfig        | 0..32               | Configurations for the SymDecrypt service . |

### 10.2.21 CalSymDecryptConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0584_Conf :</b>  |
| <b>Container Name</b>           | CalSymDecryptConfig  |
| <b>Description</b>              | Container for configuration of service SymDecrypt. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0587_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymDecryptInitConfiguration   |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                      |   |  |  |
|----------------------|---|--|--|
| <b>SWS Item</b>      | <b>CAL0586_Conf :</b>                       |  |  |
| <b>Name</b>          | CalSymDecryptPrimitiveName                  |  |  |
| <b>Description</b>   | Name of the cryptographic primitive to use. |  |  |
| <b>Multiplicity</b>  | 1   |  |  |
| <b>Type</b>          | EcucStringParamDef                          |  |  |
| <b>Default value</b> | --  |  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

#### No Included Containers

### 10.2.22 CalAsymEncrypt

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0625_Conf :</b>                                  |
| <b>Container Name</b>           | CalAsymEncrypt   |
| <b>Description</b>              | Container for incorporation of AsymEncrypt primitives. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0753_Conf :</b>  |    |              |
| <b>Name</b>               | CalAsymEncryptMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement an asymmetrical encryption. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0715_Conf :</b>  |    |              |
| <b>Name</b>               | CalAsymEncryptMaxKeySize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement an asymmetrical encryption. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                            |                     |   |
|----------------------------|---------------------|---|
| <b>Included Containers</b> |                     |   |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                   |
| CalAsymEncryptConfig       | 0..32               | Configurations for the AsymEncrypt service. |

### 10.2.23 CalAsymEncryptConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0588_Conf :</b>   |
| <b>Container Name</b>           | CalAsymEncryptConfig  |
| <b>Description</b>              | Container for configuration of service AsymEncrypt. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0591_Conf :</b>  |    |              |
| <b>Name</b>               | CalAsymEncryptInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0590_Conf :</b>                       |    |              |
| <b>Name</b>               | CalAsymEncryptPrimitiveName                 |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

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

### 10.2.24 CalAsymDecrypt

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0626_Conf :</b>                                  |
| <b>Container Name</b>           | CalAsymDecrypt   |
| <b>Description</b>              | Container for incorporation of AsymDecrypt primitives. |
| <b>Configuration Parameters</b> |  |

|                     |  |  |  |
|---------------------|--|--|--|
| <b>SWS Item</b>     | <b>CAL0754_Conf :</b>  |  |  |
| <b>Name</b>         | CalAsymDecryptMaxCtxBufByteSize  |  |  |
| <b>Description</b>  | The maximum, in bytes, of all context buffers used in all CPL primitives which implement an asymmetrical decryption. |  |  |
| <b>Multiplicity</b> | 1  |  |  |
| <b>Type</b>         | EcucIntegerParamDef  |  |  |

|                           |                         |                |
|---------------------------|-------------------------|----------------|
| <b>Range</b>              | 1 .. 4294967295         |                |
| <b>Default value</b>      | --                      |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X All Variants |
|                           | <b>Link time</b>        | --             |
|                           | <b>Post-build time</b>  | --             |
| <b>Scope / Dependency</b> | scope: module           |                |

|                           |  |                |
|---------------------------|--|----------------|
| <b>SWS Item</b>           | <b>CAL0716_Conf :</b>  |                |
| <b>Name</b>               | CalAsymDecryptMaxKeySize   |                |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement an asymmetrical decryption. |                |
| <b>Multiplicity</b>       | 1  |                |
| <b>Type</b>               | EcucIntegerParamDef  |                |
| <b>Range</b>              | 1 .. 4294967295  |                |
| <b>Default value</b>      | --   |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X All Variants |
|                           | <b>Link time</b>   | --             |
|                           | <b>Post-build time</b>   | --             |
| <b>Scope / Dependency</b> | scope: module  |                |

|                            |                     |   |
|----------------------------|---------------------|---|
| <b>Included Containers</b> |                     |   |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                   |
| CalAsymDecryptConfig       | 0..32               | Configurations for the AsymDecrypt service. |

### 10.2.25 CalAsymDecryptConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0592_Conf :</b>   |
| <b>Container Name</b>           | CalAsymDecryptConfig  |
| <b>Description</b>              | Container for configuration of service AsymDecrypt. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |                |
|---------------------------|--|----------------|
| <b>SWS Item</b>           | <b>CAL0595_Conf :</b>  |                |
| <b>Name</b>               | CalAsymDecryptInitConfiguration  |                |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |                |
| <b>Multiplicity</b>       | 1  |                |
| <b>Type</b>               | EcucStringParamDef   |                |
| <b>Default value</b>      | --   |                |
| <b>maxLength</b>          | --   |                |
| <b>minLength</b>          | --   |                |
| <b>regularExpression</b>  | --   |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X All Variants |
|                           | <b>Link time</b>   | --             |
|                           | <b>Post-build time</b>   | --             |
| <b>Scope / Dependency</b> | scope: module  |                |

|                      |   |  |
|----------------------|---|--|
| <b>SWS Item</b>      | <b>CAL0594_Conf :</b>                       |  |
| <b>Name</b>          | CalAsymDecryptPrimitiveName                 |  |
| <b>Description</b>   | Name of the cryptographic primitive to use. |  |
| <b>Multiplicity</b>  | 1   |  |
| <b>Type</b>          | EcucStringParamDef                          |  |
| <b>Default value</b> | --  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

#### No Included Containers

### 10.2.26 CalSignatureGenerate

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0627_Conf :</b>                                       |
| <b>Container Name</b>           | CalSignatureGenerate  |
| <b>Description</b>              | Container for incorporation of SignatureGenerate primitives |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0755_Conf :</b>  |    |              |
| <b>Name</b>               | CalSignatureGenerateMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a signature generation. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0717_Conf :</b>  |    |              |
| <b>Name</b>               | CalSignatureGenerateMaxKeySize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a signature generation. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                            |                     |   |
|----------------------------|---------------------|---|
| <b>Included Containers</b> |                     |   |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                         |
| CalSignatureGenerateConfig | 0..32               | Configurations for the SignatureGenerate service. |

### 10.2.27 CalSignatureGenerateConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0596_Conf :</b>   |
| <b>Container Name</b>           | CalSignatureGenerateConfig  |
| <b>Description</b>              | Container for configuration of service SignatureGenerate. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0599_Conf :</b>  |    |              |
| <b>Name</b>               | CalSignatureGenerateInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0598_Conf :</b>                       |    |              |
| <b>Name</b>               | CalSignatureGeneratePrimitiveName           |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

No Included Containers

### 10.2.28 CalSignatureVerify

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0628_Conf :</b>                                      |
| <b>Container Name</b>           | CalSignatureVerify   |
| <b>Description</b>              | Container for incorporation of SignatureVerify primitives. |
| <b>Configuration Parameters</b> |  |

|                     |  |  |  |
|---------------------|--|--|--|
| <b>SWS Item</b>     | <b>CAL0756_Conf :</b>  |  |  |
| <b>Name</b>         | CalSignatureVerifyMaxCtxBufByteSize  |  |  |
| <b>Description</b>  | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a signature verification. |  |  |
| <b>Multiplicity</b> | 1  |  |  |
| <b>Type</b>         | EcucIntegerParamDef  |  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Range</b>              | 1 .. 4294967295         |    |              |
| <b>Default value</b>      | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0718_Conf :</b>  |    |              |
| <b>Name</b>               | CalSignatureVerifyMaxKeySize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a signature verification. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                       |
| CalSignatureVerifyConfig   | 0..32               | Configurations for the SignatureVerify service. |

### 10.2.29 CalSignatureVerifyConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0600_Conf :</b>   |
| <b>Container Name</b>           | CalSignatureVerifyConfig  |
| <b>Description</b>              | Container for configuration of service SignatureVerify. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0603_Conf :</b>  |    |              |
| <b>Name</b>               | CalSignatureVerifyInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                      |   |  |  |
|----------------------|---|--|--|
| <b>SWS Item</b>      | <b>CAL0602_Conf :</b>                       |  |  |
| <b>Name</b>          | CalSignatureVerifyPrimitiveName             |  |  |
| <b>Description</b>   | Name of the cryptographic primitive to use. |  |  |
| <b>Multiplicity</b>  | 1   |  |  |
| <b>Type</b>          | EcucStringParamDef                          |  |  |
| <b>Default value</b> | --  |  |  |



|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

#### No Included Containers

### 10.2.30 CalChecksum

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0629_Conf :</b>                               |
| <b>Container Name</b>           | CalChecksum   |
| <b>Description</b>              | Container for incorporation of Checksum primitives. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0757_Conf :</b>  |    |              |
| <b>Name</b>               | CalChecksumMaxCtxBufByteSize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a checksum computation. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

| Included Containers |              |  |
|---------------------|--------------|--|
| Container Name      | Multiplicity | Scope / Dependency                       |
| CalChecksumConfig   | 0..32        | Configurations for the Checksum service. |

### 10.2.31 CalChecksumConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0604_Conf :</b>  |
| <b>Container Name</b>           | CalChecksumConfig  |
| <b>Description</b>              | Container for configuration of service Checksum. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                      |  |
|----------------------|--|
| <b>SWS Item</b>      | <b>CAL0607_Conf :</b>  |
| <b>Name</b>          | CalChecksumInitConfiguration   |
| <b>Description</b>   | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |
| <b>Multiplicity</b>  | 1  |
| <b>Type</b>          | EcucStringParamDef   |
| <b>Default value</b> | --   |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0606_Conf :</b>                       |    |              |
| <b>Name</b>               | CalChecksumPrimitiveName                    |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

No Included Containers

### 10.2.32 CalKeyDerive

|                                 |  |  |  |
|---------------------------------|--|--|--|
| <b>SWS Item</b>                 | <b>CAL0630_Conf :</b>                                |  |  |
| <b>Container Name</b>           | CalKeyDerive   |  |  |
| <b>Description</b>              | Container for incorporation of KeyDerive primitives. |  |  |
| <b>Configuration Parameters</b> |  |  |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0758_Conf :</b>  |    |              |
| <b>Name</b>               | CalKeyDeriveMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a key derivation. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                      |  |  |  |
|----------------------|--|--|--|
| <b>SWS Item</b>      | <b>CAL0719_Conf :</b>  |  |  |
| <b>Name</b>          | CalKeyDeriveMaxKeySize   |  |  |
| <b>Description</b>   | The maximum, in bytes, of all key lengths used in all CRL primitives which implement a key derivation. |  |  |
| <b>Multiplicity</b>  | 1  |  |  |
| <b>Type</b>          | EcucIntegerParamDef  |  |  |
| <b>Range</b>         | 1 .. 4294967295  |  |  |
| <b>Default value</b> | --   |  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                 |
| CalKeyDeriveConfig         | 0..32               | Configurations for the KeyDerive service. |

### 10.2.33 CalKeyDeriveConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0608_Conf :</b>   |
| <b>Container Name</b>           | CalKeyDeriveConfig  |
| <b>Description</b>              | Container for configuration of service KeyDerive. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0611_Conf :</b>  |    |              |
| <b>Name</b>               | CalKeyDeriveInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0610_Conf :</b>                       |    |              |
| <b>Name</b>               | CalKeyDerivePrimitiveName                   |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

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

### 10.2.34 CalKeyExchangeCalcPubVal

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0631_Conf :</b>  |
| <b>Container Name</b>           | CalKeyExchangeCalcPubVal   |
| <b>Description</b>              | Container for incorporation of KeyExchangeCalcPubVal primitives. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0720_Conf :</b>  |    |              |
| <b>Name</b>               | CalKeyExchangeCalcPubValMaxBaseTypeSize  |    |              |
| <b>Description</b>        | The maximum length, in bytes, of all base types used in all CPL primitives which implement a public value calculation. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                    |  |    |              |
|--------------------|--|----|--------------|
| SWS Item           | CAL0759_Conf :   |    |              |
| Name               | CalKeyExchangeCalcPubValMaxCtxBufByteSize  |    |              |
| Description        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a public value calculation. |    |              |
| Multiplicity       | 1  |    |              |
| Type               | EcucIntegerParamDef  |    |              |
| Range              | 1 .. 4294967295  |    |              |
| Default value      | --   |    |              |
| ConfigurationClass | Pre-compile time   | X  | All Variants |
|                    | Link time  | -- |              |
|                    | Post-build time  | -- |              |
| Scope / Dependency | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0721_Conf :</b>   |    |              |
| <b>Name</b>               | CalKeyExchangeCalcPubValMaxPrivateTypeSize  |    |              |
| <b>Description</b>        | The maximum length, in bytes, of all private information types used in all CPL primitives which implement a public value calculation. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucIntegerParamDef   |    |              |
| <b>Range</b>              | 1 .. 4294967295   |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>   | X  | All Variants |
|                           | <b>Link time</b>  | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module   |    |              |

| <b>Included Containers</b>     |                     |  |
|--------------------------------|---------------------|--|
| <b>Container Name</b>          | <b>Multiplicity</b> | <b>Scope / Dependency</b>                    |
| CalKeyExchangeCalcPubValConfig | 0..32               | Configurations for the KeyExchangeCalcPubVal |

## 10.2.35 CalKeyExchangeCalcPubValConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0612_Conf :</b>   |
| <b>Container Name</b>           | CalKeyExchangeCalcPubValConfig  |
| <b>Description</b>              | Container for configuration of service KeyExchangeCalcPubVal. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0615_Conf :</b>  |    |              |
| <b>Name</b>               | CalKeyExchangeCalcPubValInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0614_Conf :</b>                       |    |              |
| <b>Name</b>               | CalKeyExchangeCalcPubValPrimitiveName       |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

No Included Containers

## 10.2.36 CalKeyExchangeCalcSecret

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0632_Conf :</b>  |
| <b>Container Name</b>           | CalKeyExchangeCalcSecret   |
| <b>Description</b>              | Container for incorporation of KeyExchangeCalcSecret primitives. |
| <b>Configuration Parameters</b> |  |

|                     |   |
|---------------------|---|
| <b>SWS Item</b>     | <b>CAL0722_Conf :</b>   |
| <b>Name</b>         | CalKeyExchangeCalcSecretMaxBaseTypeSize   |
| <b>Description</b>  | The maximum length, in bytes, of all base types used in all CPL primitives which implement a shared secret calculation. |
| <b>Multiplicity</b> | 1   |
| <b>Type</b>         | EcucIntegerParamDef   |

|                           |                         |                |
|---------------------------|-------------------------|----------------|
| <b>Range</b>              | 1 .. 4294967295         |                |
| <b>Default value</b>      | --                      |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X All Variants |
|                           | <b>Link time</b>        | --             |
|                           | <b>Post-build time</b>  | --             |
| <b>Scope / Dependency</b> | scope: module           |                |

|                           |   |                |
|---------------------------|---|----------------|
| <b>SWS Item</b>           | <b>CAL0760_Conf :</b>   |                |
| <b>Name</b>               | CalKeyExchangeCalcSecretMaxCtxBufByteSize   |                |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a shared secret calculation. |                |
| <b>Multiplicity</b>       | 1   |                |
| <b>Type</b>               | EcucIntegerParamDef   |                |
| <b>Range</b>              | 1 .. 4294967295   |                |
| <b>Default value</b>      | --  |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>   | X All Variants |
|                           | <b>Link time</b>  | --             |
|                           | <b>Post-build time</b>  | --             |
| <b>Scope / Dependency</b> | scope: module   |                |

|                           |  |                |
|---------------------------|--|----------------|
| <b>SWS Item</b>           | <b>CAL0723_Conf :</b>  |                |
| <b>Name</b>               | CalKeyExchangeCalcSecretMaxPrivateTypeSize   |                |
| <b>Description</b>        | The maximum length, in bytes, of all private information types used in all CPL primitives which implement a shared secret calculation. |                |
| <b>Multiplicity</b>       | 1  |                |
| <b>Type</b>               | EcucIntegerParamDef  |                |
| <b>Range</b>              | 1 .. 4294967295  |                |
| <b>Default value</b>      | --   |                |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X All Variants |
|                           | <b>Link time</b>   | --             |
|                           | <b>Post-build time</b>   | --             |
| <b>Scope / Dependency</b> | scope: module  |                |

|                                |                     |   |
|--------------------------------|---------------------|---|
| <b>Included Containers</b>     |                     |   |
| <b>Container Name</b>          | <b>Multiplicity</b> | <b>Scope / Dependency</b>                             |
| CalKeyExchangeCalcSecretConfig | 0..32               | Configurations for the KeyExchangeCalcSecret service. |

### 10.2.37 CalKeyExchangeCalcSecretConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0616_Conf :</b>   |
| <b>Container Name</b>           | CalKeyExchangeCalcSecretConfig  |
| <b>Description</b>              | Container for configuration of service KeyExchangeCalcSecret. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                     |  |  |
|---------------------|--|--|
| <b>SWS Item</b>     | <b>CAL0545_Conf :</b>  |  |
| <b>Name</b>         | CalKeyExchangeCalcSecretInitConfiguration  |  |
| <b>Description</b>  | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |  |
| <b>Multiplicity</b> | 1  |  |
| <b>Type</b>         | EcucStringParamDef   |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Default value</b>      | --                      |    |              |
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0618_Conf :</b>                       |    |              |
| <b>Name</b>               | CalKeyExchangeCalcSecretPrimitiveName       |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

**No Included Containers**

### 10.2.38 CalSymKeyExtract

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0633_Conf :</b>                                    |
| <b>Container Name</b>           | CalSymKeyExtract   |
| <b>Description</b>              | Container for incorporation of SymKeyExtract primitives. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0761_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymKeyExtractMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement a symmetrical key extraction. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                     |  |  |  |
|---------------------|--|--|--|
| <b>SWS Item</b>     | <b>CAL0724_Conf :</b>  |  |  |
| <b>Name</b>         | CalSymKeyExtractMaxKeySize   |  |  |
| <b>Description</b>  | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a symmetrical key extraction. |  |  |
| <b>Multiplicity</b> | 1  |  |  |
| <b>Type</b>         | EcucIntegerParamDef  |  |  |
| <b>Range</b>        | 1 .. 4294967295  |  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Default value</b>      | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

| <b>Included Containers</b> |                     |   |
|----------------------------|---------------------|---|
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>                     |
| CalSymKeyExtractConfig     | 0..32               | Configurations for the SymKeyExtract service. |

### 10.2.39 CalSymKeyExtractConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0546_Conf :</b>   |
| <b>Container Name</b>           | CalSymKeyExtractConfig  |
| <b>Description</b>              | Container for configuration of service SymKeyExtract. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0549_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymKeyExtractInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0548_Conf :</b>                       |    |              |
| <b>Name</b>               | CalSymKeyExtractPrimitiveName               |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

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



#### 10.2.40 CalAsymPublicKeyExtract

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0634_Conf :</b>   |
| <b>Container Name</b>           | CalAsymPublicKeyExtract   |
| <b>Description</b>              | Container for incorporation of AsymPublicKeyExtract primitives. |
| <b>Configuration Parameters</b> |   |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0762_Conf :</b>   |    |              |
| <b>Name</b>               | CalAsymPublicKeyExtractMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement an asymmetrical public key extraction. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucIntegerParamDef   |    |              |
| <b>Range</b>              | 1 .. 4294967295   |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>   | X  | All Variants |
|                           | <b>Link time</b>  | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module   |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0725_Conf :</b>   |    |              |
| <b>Name</b>               | CalAsymPublicKeyExtractMaxKeySize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement an asymmetrical public key extraction. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucIntegerParamDef   |    |              |
| <b>Range</b>              | 1 .. 4294967295   |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>   | X  | All Variants |
|                           | <b>Link time</b>  | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module   |    |              |

|                               |                     |  |
|-------------------------------|---------------------|--|
| <b>Included Containers</b>    |                     |  |
| <b>Container Name</b>         | <b>Multiplicity</b> | <b>Scope / Dependency</b>                            |
| CalAsymPublicKeyExtractConfig | 0..32               | Configurations for the AsymPublicKeyExtract service. |

#### 10.2.41 CalAsymPublicKeyExtractConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0550_Conf :</b>  |
| <b>Container Name</b>           | CalAsymPublicKeyExtractConfig  |
| <b>Description</b>              | Container for configuration of service AsymPublicKeyExtract. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                     |  |
|---------------------|--|
| <b>SWS Item</b>     | <b>CAL0553_Conf :</b>  |
| <b>Name</b>         | CalAsymPublicKeyExtractInitConfiguration   |
| <b>Description</b>  | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |
| <b>Multiplicity</b> | 1  |
| <b>Type</b>         | EcucStringParamDef   |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Default value</b>      | --                      |    |              |
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0552_Conf :</b>                       |    |              |
| <b>Name</b>               | CalAsymPublicKeyExtractPrimitiveName        |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

**No Included Containers**

#### 10.2.42 CalAsymPrivateKeyExtract

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0686_Conf :</b>  |
| <b>Container Name</b>           | CalAsymPrivateKeyExtract   |
| <b>Description</b>              | Container for incorporation of AsymPrivateKeyExtract primitives. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0763_Conf :</b>  |    |              |
| <b>Name</b>               | CalAsymPrivateKeyExtractMaxCtxBufByteSize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all context buffers used in all CPL primitives which implement an asymmetrical private key extraction. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                     |  |  |  |
|---------------------|--|--|--|
| <b>SWS Item</b>     | <b>CAL0726_Conf :</b>  |  |  |
| <b>Name</b>         | CalAsymPrivateKeyExtractMaxKeySize   |  |  |
| <b>Description</b>  | The maximum, in bytes, of all key lengths used in all CPL primitives which implement an asymmetrical private key extraction. |  |  |
| <b>Multiplicity</b> | 1  |  |  |
| <b>Type</b>         | EcucIntegerParamDef  |  |  |
| <b>Range</b>        | 1 .. 4294967295  |  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Default value</b>      | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

| <b>Included Containers</b>     |                     |   |
|--------------------------------|---------------------|---|
| <b>Container Name</b>          | <b>Multiplicity</b> | <b>Scope / Dependency</b>                     |
| CalAsymPrivateKeyExtractConfig | 0..32               | Configurations for the AsymPrivateKeyExtract. |

### 10.2.43 CalAsymPrivateKeyExtractConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0687_Conf :</b>   |
| <b>Container Name</b>           | CalAsymPrivateKeyExtractConfig  |
| <b>Description</b>              | Container for configuration of service AsymPrivateKeyExtract. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0690_Conf :</b>  |    |              |
| <b>Name</b>               | CalAsymPrivateKeyExtractInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0689_Conf :</b>                       |    |              |
| <b>Name</b>               | CalAsymPrivateKeyExtractPrimitiveName       |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

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

### 10.2.44 CalSymKeyWrapAsym

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0765_Conf :</b>                                     |
| <b>Container Name</b>           | CalSymKeyWrapAsym   |
| <b>Description</b>              | Container for incorporation of SymKeyWrapAsym primitives. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0785_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymKeyWrapAsymMaxPubKeySize   |    |              |
| <b>Description</b>        | The maximum length, in bytes, of all public key types used in all CPL primitives which implement a symmetrical key wrapping. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0786_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymKeyWrapAsymMaxSymKeySize   |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a symmetrical key wrapping. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                            |                     |  |
|----------------------------|---------------------|--|
| <b>Included Containers</b> |                     |  |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>  |
| CalSymKeyWrapAsymConfig    | 0..32               | Container for configuration of service SymKeyWrapAsym. The container name serves as a symbolic name for the identifier of a service configuration. |

### 10.2.45 CalSymKeyWrapAsymConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0782_Conf :</b>  |
| <b>Container Name</b>           | CalSymKeyWrapAsymConfig  |
| <b>Description</b>              | Container for configuration of service SymKeyWrapAsym. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                     |  |
|---------------------|--|
| <b>SWS Item</b>     | <b>CAL0784_Conf :</b>  |
| <b>Name</b>         | CalSymKeyWrapAsymInitConfiguration   |
| <b>Description</b>  | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |
| <b>Multiplicity</b> | 1  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Type</b>               | EcucStringParamDef      |    |              |
| <b>Default value</b>      | --                      |    |              |
| <b>maxLength</b>          | --                      |    |              |
| <b>minLength</b>          | --                      |    |              |
| <b>regularExpression</b>  | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0783_Conf :</b>                       |    |              |
| <b>Name</b>               | CalSymKeyWrapAsymPrimitiveName              |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

#### No Included Containers

### 10.2.46 CalSymKeyWrapSym

|                                 |  |  |  |
|---------------------------------|--|--|--|
| <b>SWS Item</b>                 | <b>CAL0764_Conf :</b>                                    |  |  |
| <b>Container Name</b>           | CalSymKeyWrapSym   |  |  |
| <b>Description</b>              | Container for incorporation of SymKeyWrapSym primitives. |  |  |
| <b>Configuration Parameters</b> |  |  |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0781_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymKeyWrapSymMaxSymKeySize  |    |              |
| <b>Description</b>        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement a symmetrical key wrapping. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                            |                     |   |
|----------------------------|---------------------|---|
| <b>Included Containers</b> |                     |   |
| <b>Container Name</b>      | <b>Multiplicity</b> | <b>Scope / Dependency</b>   |
| CalSymKeyWrapSymConfig     | 0..32               | Container for configuration of service SymKeyWrapSym. The container name serves as a symbolic name for the identifier of a service configuration. |

### 10.2.47 CalSymKeyWrapSymConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0777_Conf :</b>   |
| <b>Container Name</b>           | CalSymKeyWrapSymConfig  |
| <b>Description</b>              | Container for configuration of service SymKeyWrapSym. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0779_Conf :</b>  |    |              |
| <b>Name</b>               | CalSymKeyWrapSymInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0778_Conf :</b>                       |    |              |
| <b>Name</b>               | CalSymKeyWrapSymPrimitiveName               |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

**No Included Containers**

### 10.2.48 CalAsymPrivateKeyWrapAsym

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0767_Conf :</b>   |
| <b>Container Name</b>           | CalAsymPrivateKeyWrapAsym   |
| <b>Description</b>              | Container for incorporation of AsymPrivateKeyWrapAsym primitives. |
| <b>Configuration Parameters</b> |   |

|                     |   |  |  |
|---------------------|---|--|--|
| <b>SWS Item</b>     | <b>CAL0771_Conf :</b>   |  |  |
| <b>Name</b>         | CalAsymPrivateKeyWrapAsymMaxPrivKeySize   |  |  |
| <b>Description</b>  | The maximum length, in bytes, of all private information types used in all CPL primitives which implement an asymmetrical key wrapping. |  |  |
| <b>Multiplicity</b> | 1   |  |  |
| <b>Type</b>         | EcucIntegerParamDef   |  |  |

|                           |                         |    |              |
|---------------------------|-------------------------|----|--------------|
| <b>Range</b>              | 1 .. 4294967295         |    |              |
| <b>Default value</b>      | --                      |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b> | X  | All Variants |
|                           | <b>Link time</b>        | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module           |    |              |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0787_Conf :</b>  |    |              |
| <b>Name</b>               | CalAsymPrivateKeyWrapAsymMaxPubKeySize   |    |              |
| <b>Description</b>        | The maximum length, in bytes, of all public key types used in all CPL primitives which implement an asymmetrical key wrapping. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucIntegerParamDef  |    |              |
| <b>Range</b>              | 1 .. 4294967295  |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

| <b>Included Containers</b>      |                     |  |
|---------------------------------|---------------------|--|
| <b>Container Name</b>           | <b>Multiplicity</b> | <b>Scope / Dependency</b>  |
| CalAsymPrivateKeyWrapAsymConfig | 0..32               | Container for configuration of service AsymPrivateKeyWrapAsym. The container name serves as a symbolic name for the identifier of a service configuration. |

### 10.2.49 CalAsymPrivateKeyWrapAsymConfig

|                                 |  |
|---------------------------------|--|
| <b>SWS Item</b>                 | <b>CAL0768_Conf :</b>  |
| <b>Container Name</b>           | CalAsymPrivateKeyWrapAsymConfig  |
| <b>Description</b>              | Container for configuration of service AsymPrivateKeyWrapAsym. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |  |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0770_Conf :</b>  |    |              |
| <b>Name</b>               | CalAsymPrivateKeyWrapAsymInitConfiguration   |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |



|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0769_Conf :</b>                       |    |              |
| <b>Name</b>               | CalAsymPrivateKeyWrapAsymPrimitiveName      |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

**No Included Containers**

### 10.2.50 CalAsymPrivateKeyWrapSym

|                                 |  |  |  |
|---------------------------------|--|--|--|
| <b>SWS Item</b>                 | <b>CAL0766_Conf :</b>  |  |  |
| <b>Container Name</b>           | CalAsymPrivateKeyWrapSym   |  |  |
| <b>Description</b>              | Container for incorporation of AsymPrivateKeyWrapSym primitives. |  |  |
| <b>Configuration Parameters</b> |  |  |  |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0775_Conf :</b>   |    |              |
| <b>Name</b>               | CalAsymPrivateKeyWrapSymMaxPrivKeySize  |    |              |
| <b>Description</b>        | The maximum length, in bytes, of all private information types used in all CPL primitives which implement an asymmetrical key wrapping. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucIntegerParamDef   |    |              |
| <b>Range</b>              | 1 .. 4294967295   |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>   | X  | All Variants |
|                           | <b>Link time</b>  | -- |              |
|                           | <b>Post-build time</b>  | -- |              |
| <b>Scope / Dependency</b> | scope: module   |    |              |

|                    |  |    |              |
|--------------------|--|----|--------------|
| SWS Item           | CAL0776_Conf :   |    |              |
| Name               | CalAsymPrivateKeyWrapSymMaxSymKeySize  |    |              |
| Description        | The maximum, in bytes, of all key lengths used in all CPL primitives which implement an asymmetrical key wrapping. |    |              |
| Multiplicity       | 1  |    |              |
| Type               | EcucIntegerParamDef  |    |              |
| Range              | 1 .. 4294967295  |    |              |
| Default value      | --   |    |              |
| ConfigurationClass | Pre-compile time   | X  | All Variants |
|                    | Link time  | -- |              |
|                    | Post-build time  | -- |              |
| Scope / Dependency | scope: module  |    |              |

**Included Containers**



| Container Name                 | Multiplicity | Scope / Dependency  |
|--------------------------------|--------------|---|
| CalAsymPrivateKeyWrapSymConfig | 0..32        | Container for configuration of service AsymPrivateKeyWrapSym. The container name serves as a symbolic name for the identifier of a service configuration. |

### 10.2.51 CalAsymPrivateKeyWrapSymConfig

|                                 |   |
|---------------------------------|---|
| <b>SWS Item</b>                 | <b>CAL0772 Conf :</b>   |
| <b>Container Name</b>           | CalAsymPrivateKeyWrapSymConfig  |
| <b>Description</b>              | Container for configuration of service AsymPrivateKeyWrapSym. The container name serves as a symbolic name for the identifier of a service configuration. |
| <b>Configuration Parameters</b> |   |

|                           |  |    |              |
|---------------------------|--|----|--------------|
| <b>SWS Item</b>           | <b>CAL0774_Conf :</b>  |    |              |
| <b>Name</b>               | CalAsymPrivateKeyWrapSymInitConfiguration  |    |              |
| <b>Description</b>        | Name of a C symbol which contains the configuration of the underlying cryptographic primitive. |    |              |
| <b>Multiplicity</b>       | 1  |    |              |
| <b>Type</b>               | EcucStringParamDef   |    |              |
| <b>Default value</b>      | --   |    |              |
| <b>maxLength</b>          | --   |    |              |
| <b>minLength</b>          | --   |    |              |
| <b>regularExpression</b>  | --   |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>  | X  | All Variants |
|                           | <b>Link time</b>   | -- |              |
|                           | <b>Post-build time</b>   | -- |              |
| <b>Scope / Dependency</b> | scope: module  |    |              |

|                           |   |    |              |
|---------------------------|---|----|--------------|
| <b>SWS Item</b>           | <b>CAL0773_Conf :</b>                       |    |              |
| <b>Name</b>               | CalAsymPrivateKeyWrapSymPrimitiveName       |    |              |
| <b>Description</b>        | Name of the cryptographic primitive to use. |    |              |
| <b>Multiplicity</b>       | 1   |    |              |
| <b>Type</b>               | EcucStringParamDef                          |    |              |
| <b>Default value</b>      | --  |    |              |
| <b>maxLength</b>          | --  |    |              |
| <b>minLength</b>          | --  |    |              |
| <b>regularExpression</b>  | --  |    |              |
| <b>ConfigurationClass</b> | <b>Pre-compile time</b>                     | X  | All Variants |
|                           | <b>Link time</b>                            | -- |              |
|                           | <b>Post-build time</b>                      | -- |              |
| <b>Scope / Dependency</b> | scope: module                               |    |              |

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

### 10.3 Published Information

[CAL0756] 「 The standardized common published parameters as required by BSW00402 in the General Requirements on Basic Software Modules [3] shall be published within the header file of this module and need to be provided in the BSW Module Description. The according module abbreviation can be found in the List of Basic Software Modules [1]. 」()

Additional module-specific published parameters are listed below if applicable.

## 11 Not applicable requirements

**[CAL9999]** 「 These requirements are not applicable to this specification. 」  
(BSW00411)