

<b>Document Title</b>	Specification of Crypto Driver
<b>Document Owner</b>	AUTOSAR
<b>Document Responsibility</b>	AUTOSAR
<b>Document Identification No</b>	807

<b>Document Status</b>	published
<b>Part of AUTOSAR Standard</b>	Classic Platform
<b>Part of Standard Release</b>	R19-11

<b>Document Change History</b>			
<b>Date</b>	<b>Release</b>	<b>Changed by</b>	<b>Change Description</b>
2019-11-28	R19-11	AUTOSAR Release Management	<ul style="list-style-type: none"> <li>• Minor corrections and editorial changes</li> <li>• Cleanup of return code and DET error</li> <li>• Default RNG configuration for CryptoDriver Objects</li> <li>• Clarification on Read/Write access for key element.</li> <li>• Remove certificate support functions</li> <li>• Remove virtual key references</li> <li>• Changed Document Status from Final to published</li> </ul>
2018-10-31	4.4.0	AUTOSAR Release Management	<ul style="list-style-type: none"> <li>• Remove secure counter</li> <li>• Align return values of interface functions.</li> <li>• Support source and destination buffers for crypto operations located in crypto driver.</li> <li>• Support key management operation in asynchronous mode</li> </ul>
2017-12-08	4.3.1	AUTOSAR Release Management	<ul style="list-style-type: none"> <li>• Rollout of 'Runtime Errors'</li> <li>• minor corrections, clarifications and editorial changes; For details please refer to the ChangeDocumentation</li> </ul>
2016-11-30	4.3.0	AUTOSAR Release Management	<ul style="list-style-type: none"> <li>• Initial Release</li> </ul>

		SWS_Crypto_91011, SWS_Crypto_00168, -SWS_Crypto_00169, -SWS_Crypto_00170, -SWS_Crypto_00171, -SWS_Crypto_00172, SWS_Crypto_00173, -SWS_Crypto_00174, -SWS_Crypto_00175, -SWS_Crypto_00176, -SWS_Crypto_00177, -SWS_Crypto_00178, ~ECUC_Crypto_00041).
		SWS_Crypto_00142
		SWS_Crypto_91000

## Disclaimer

This work (specification and/or software implementation) and the material contained in it, as released by AUTOSAR, is for the purpose of information only. AUTOSAR and the companies that have contributed to it shall not be liable for any use of the work.

The material contained in this work is protected by copyright and other types of intellectual property rights. The commercial exploitation of the material contained in this work requires a license to such intellectual property rights.

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

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

The word AUTOSAR and the AUTOSAR logo are registered trademarks.

## Table of Contents

1	Introduction and functional overview .....	6
2	Acronyms and abbreviations .....	7
2.1	Glossary of Terms .....	7
3	Related documentation.....	9
3.1	Input documents.....	9
3.2	Related standards and norms .....	9
3.3	Related specification .....	9
4	Constraints and assumptions .....	10
4.1	Limitations .....	10
4.2	Applicability to car domains.....	10
5	Dependencies to other modules.....	11
5.1	File structure .....	11
5.1.1	Code File Structure .....	11
6	Requirements traceability .....	12
7	Functional specification .....	13
7.1	Pre-Configuration .....	13
7.1.1	Cryptographic capabilities.....	14
7.1.2	Available Keys .....	14
7.2	General Behavior .....	15
7.2.1	Normal Operation.....	16
7.2.2	Functional Requirements .....	19
7.2.3	Design Notes .....	19
7.2.4	Key Management.....	21
7.2.5	Key Formats.....	23
7.3	Error classification .....	27
7.3.1	Development Errors .....	27
7.3.2	Runtime Errors.....	27
7.3.3	Transient Faults .....	27
7.3.4	Production Errors.....	28
7.3.5	Extended Production Errors.....	28
7.4	Error detection.....	28
8	API specification.....	29
8.1	Imported types.....	29
8.2	Type Definitions.....	30
8.3	Function definitions .....	30
8.3.1	General API .....	31
8.3.2	Job Processing Interface .....	32
8.3.3	Job Cancellation Interface .....	38
8.3.4	Key Management Interface.....	40
8.4	Scheduled functions.....	58
8.5	Expected Interfaces.....	59

8.5.1	Interfaces to Standard Software Modules .....	59
8.5.2	Mandatory Interfaces .....	59
8.5.3	Optional Interfaces.....	59
9	Sequence diagrams .....	60
10	Configuration specification.....	61
10.1	Containers and configuration parameters .....	61
10.1.1	Crypto .....	61
10.1.2	CryptoGeneral .....	62
10.1.3	CryptoDriverObjects .....	64
10.1.4	CryptoDriverObject .....	65
10.1.5	CryptoKeys .....	68
10.1.6	CryptoKey.....	69
10.1.7	CryptoKeyElements .....	70
10.1.8	CryptoKeyElement.....	72
10.1.9	CryptoKeyTypes .....	75
10.1.10	CryptoKeyType .....	75
10.1.11	CryptoPrimitives .....	76
10.1.12	CryptoPrimitive .....	77
10.2	Published Information.....	83

## 1 Introduction and functional overview

This specification specifies the functionality, API and the configuration of the AUTOSAR Basic Software module Crypto Driver.

The Crypto Drivers are located in the Microcontroller Abstraction Layer, which is below the Crypto Hardware Abstraction Layer (Crypto Interface [4]) and the upper service layer (Crypto Service Manager [5]). The Crypto Driver is a driver for a specific device, that is only abstracting the features supported by the hardware.

The Crypto Drivers allow defining of different Crypto Driver Objects (i.e. AES accelerator, SW component, etc), which shall be used for concurrent requests in different buffers. For each hardware object a priority-dependent job processing shall be supported. A crypto software solution (i.e. software-based CDD) can define interfaces identical to the Crypto Drivers for interacting with the upper layers, which shall provide an interface to the applications.

## 2 Acronyms and abbreviations

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

### 2.1 Glossary of Terms

<b>Terms:</b>	<b>Description:</b>		
Crypto Driver Object	A Crypto Driver implements one or more Crypto Driver Objects. The Crypto Driver Object can offer different crypto primitives in hardware or software. The Crypto Driver Objects of one Crypto Driver are independent of each other. There is only one workspace for each Crypto Driver Object (i.e. only one crypto primitive can be performed at the same time)		
Key	A Key can be referenced by a job in the Csm. In the Crypto Driver, the key references a specific key type.		
Key Type	A key type consists of references to key elements. The key types are typically pre-configured by the vendor of the Crypto Driver.		
Key Element	Key elements are used to store data. This data can be e.g. key material or the IV needed for AES encryption. It can also be used to configure the behaviour of the key management functions.		
Channel	A channel is the path from a Crypto Service Manager queue via the Crypto Interface to a specific Crypto Driver Object.		
Job	A 'Job' is a configured 'CsmJob'. Among others, it refers to a key, a cryptographic primitive and a reference channel.		
Crypto Primitive	'Primitive' is an instance of a configured cryptographic algorithm realized in a Crypto Driver Object. Among others it refers to a functionality provided by the CSM to the application, the concrete underlining 'algorithmfamily' (e.g. AES, MD5, RSA, ...), and a 'algorithmmode' (e.g. ECB, CBC, ...).		
Operation	An operation of a crypto primitive declares what part of the crypto primitive shall be performed. There are three different operation modes: <table border="1" data-bbox="432 1966 1412 2072"> <tr> <td>START</td> <td>Operation mode indicates a new request of a crypto primitive, and it shall cancel all previous requests of the same job and primitive.</td> </tr> </table>	START	Operation mode indicates a new request of a crypto primitive, and it shall cancel all previous requests of the same job and primitive.
START	Operation mode indicates a new request of a crypto primitive, and it shall cancel all previous requests of the same job and primitive.		

	UPDATE	Operation mode indicates, that the crypto primitive expects input data.
	FINISH	Operation mode indicates, that after this part all data are fed completely and the crypto primitive can finalize the calculations.
	It is also possible to perform more than one operation at once by concatenating the corresponding bits of the operation mode argument.	
Priority	The priority of a job defines the importance of it. The higher the priority (as well in value), the more immediate the job will be executed. The priority of a cryptographic job is part of the configuration.	
Service	A 'Service' shall be understood as defined in the TR_Glossary document: A service is a type of operation that has a published specification of interface and behavior, involving a contract between the provider of the capability and the potential clients.	



## 3 Related documentation

### 3.1 Input documents

- [1] AUTOSAR Layered Software Architecture  
AUTOSAR\_EXP\_LayeredSoftwareArchitecture.pdf
- [2] AUTOSAR General Requirements on Basic Software Modules  
AUTOSAR\_SRS\_BSWGeneral.pdf
- [3] AUTOSAR General Specification for Basic Software Modules  
AUTOSAR\_SWS\_BSWGeneral.pdf
- [4] AUTOSAR Specification of Crypto Interface  
AUTOSAR\_SWS\_CryptoInterface.pdf
- [5] AUTOSAR Specification of Crypto Service Manager  
AUTOSAR\_SWS\_CryptoServiceManager.pdf
- [6] AUTOSAR Requirements on Crypto Modules  
AUTOSAR\_SRS\_CryptoStack.pdf
- [7] Glossary  
AUTOSAR\_TR\_Glossary

### 3.2 Related standards and norms

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

### 3.3 Related specification

AUTOSAR provides a General Specification on Basic Software (SWS BSW General) [3] which is also valid for Crypto Driver

Thus, the specification SWS BSW General [3] shall be considered as additional and required specification for Crypto Driver.

## 4 Constraints and assumptions

### 4.1 Limitations

n.a.

### 4.2 Applicability to car domains

The Crypto Driver can be used for all domain applications when security features are to be used.

## 5 Dependencies to other modules

**[SWS\_Crypto\_00003]** [ If an off-chip crypto hardware module (e.g. external HSM) is used, the Crypto Driver shall use services of other MCAL drivers (e.g. SPI).  
]

Hint: If the Crypto Driver uses services of other MCAL drivers (e.g. SPI), it must be ensured that these drivers are up and running before initializing the Crypto Driver module.

**[SWS\_Crypto\_00116]** [The Crypto Driver shall be able to store key material in a non-volatile way if supported by the dedicated crypto hardware.  
]

Note:

The Crypto Drivers are called by the Crypto Interface (CRYIF), which is implemented according to the cryptographic interface specification [4].

The Crypto Drivers access the underlying hardware and software objects, to calculate results with their cryptographic primitives. The results shall be forwarded to the CRYIF.

### 5.1 File structure

#### 5.1.1 Code File Structure

The code file structure is not defined within this specification completely.

**[SWS\_Crypto\_00005]** [ The code file structure shall contain a source file Crypto.c and a code file Crypto\_KeyManagement.c.  
]

()

## 6 Requirements traceability

Requirement	Description	Satisfied by
SRS_BSW_00101	The Basic Software Module shall be able to initialize variables and hardware in a separate initialization function	SWS_Crypto_91000
SRS_BSW_00358	The return type of init() functions implemented by AUTOSAR Basic Software Modules shall be void	SWS_Crypto_91000
SRS_BSW_00407	Each BSW module shall provide a function to read out the version information of a dedicated module implementation	SWS_Crypto_91001
SRS_BSW_00414	Init functions shall have a pointer to a configuration structure as single parameter	SWS_Crypto_91000
SRS_CryptoStack_00008	The Crypto Stack shall allow static configuration of keys used for cryptographic jobs	SWS_Crypto_00184, SWS_Crypto_00185, SWS_Crypto_00186, SWS_Crypto_00187, SWS_Crypto_00188, SWS_Crypto_00189, SWS_Crypto_00190, SWS_Crypto_00191, SWS_Crypto_00192, SWS_Crypto_00193
SRS_CryptoStack_00086	The CSM module shall distinguish between error types	SWS_Crypto_00040
SRS_CryptoStack_00098	The Crypto Driver shall provide access to all cryptographic algorithms supported by the hardware	SWS_Crypto_00013
SWS_BSW_00050	Check parameters passed to Initialization functions	SWS_Crypto_00215
SWS_BSW_00216	-	SWS_Crypto_91016

## 7 Functional specification

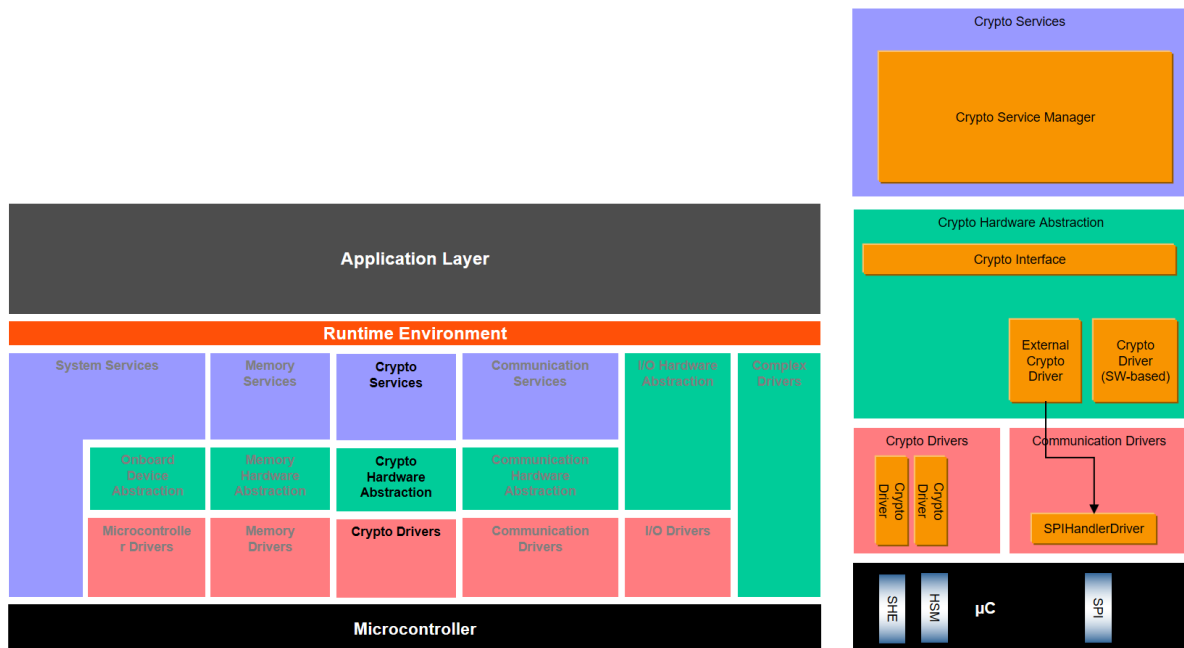


Figure 7.1: AUTOSAR Layered View with Crypto Driver Module

The Crypto Driver module is located in the micro controller abstraction layer and is below the Crypto Interface module and Crypto Service Manager module. It implements a generic interface for synchronous and asynchronous cryptographic primitives. It also supports key storage, key configuration, and key management for cryptographic services.

To provide cryptographic functionalities an ECU needs to integrate one unique Crypto Service Manager module and one Crypto Interface. However, the Crypto Interface can access several Crypto Drivers, each of them is configured according to the underlying Crypto Driver Object.

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

### 7.1 Pre-Configuration

The vendor of the Crypto Driver has to provide a pre-configuration for the Crypto Driver which represents the capabilities of the Crypto Driver. The pre-configuration shall be delivered with the BSWMD-file of the Crypto Driver.

### 7.1.1 Cryptographic capabilities

The capabilities of a Crypto Driver can be divided in the two main topics: key storage and supported algorithms. The supported algorithms can be pre-configured by creating a new CryptoPrimitive container (e.g. MacGenerate). In this container the vendor can now specify that the Crypto Driver is for example only capable of doing a CMAC. In this case, an example configuration would be:

```
CryptoPrimitiveAlgorithmFamily = CRYPTO_ALGOFAM_AES  
CryptoPrimitiveAlgorithmMode = CRYPTO_ALGOMODE_CMAC  
CryptoPrimitiveAlgorithmSecondaryFamily =  
CRYPTO_ALGOMODE_NOT_SET  
CryptoPrimitiveService = MacGenerate
```

The primitive MacGenerate can then be referenced by the Crypto Driver Object to show, that it is capable of doing a CMAC. If no other primitives are pre-configured, the Crypto Driver Object is not able to perform e.g. an AES encryption.

If all primitives are independent from each other, a vendor would pre-configure one Crypto Driver Object for each primitive. Otherwise, there would be one Crypto Driver Object, which would reference all primitives.

### 7.1.2 Available Keys

The keys, which are provided by the Crypto Driver can also be pre-configured. A CryptoKey container references a specific CryptoKeyType. The CryptoKeyType provides the information which key elements are contained in a CryptoKey referencing this CryptoKeyType.

The vendor also pre-configures the key elements to define:

- read/write access
- the maximum size of the element
- if the element can be read/written with data smaller than the maximum size
- the init value after startup if the element is not already initialized

The init value is the value, which is stored into the key element at the initialization of the crypto driver when the key element is empty. It is e.g. used for the key element with the id CRYPTO\_KE\_<Service>\_ALGORITHM. This way, the key management functions can be configured. To provide e.g. different key exchange algorithms in one Crypto Driver, the vendor can pre-configure the following containers and set the init values of the CRYPTO\_KE\_<Service>\_ALGORITHM key element to a vendor specific value:

CryptoKeyElement\_KeyExchange\_Algorithm\_RSA

- ID = 11
- Init value = 0x00
- Size = 1
- Read Access = RA\_NONE
- Write Access = WA\_NONE

CryptoKeyElement\_KeyExchange\_Algorithm\_Ed25519

- ID = 11
- Init value = 0x01
- Size = 1
- Read Access = RA\_NONE
- Write Access = WA\_NONE

CryptoKeyType\_KeyExchange\_RSA

- CryptoKeyElement\_KeyExchange\_Algorithm\_RSA
- CryptoKeyElement\_KeyExchange\_PartnerPubKey
- CryptoKeyElement\_KeyExchange\_OwnPubKey
- CryptoKeyElement\_KeyExchange\_Base
- CryptoKeyElement\_KeyExchange\_PrivKey
- CryptoKeyElement\_KeyExchange\_SharedValue

CryptoKeyType\_KeyExchange\_Ed25519

- CryptoKeyElement\_KeyExchange\_Algorithm\_Ed25519
- CryptoKeyElement\_KeyExchange\_PartnerPubKey
- CryptoKeyElement\_KeyExchange\_OwnPubKey
- CryptoKeyElement\_KeyExchange\_Base
- CryptoKeyElement\_KeyExchange\_PrivKey
- CryptoKeyElement\_KeyExchange\_SharedValue

When a key exchange should be performed with a CryptoKey of type CryptoKeyType\_KeyExchange\_Ed25519, the Crypto Driver knows with the value stored in the key element CRYPTO\_KE\_KEYEXCHANGE\_ALGORITHM that Ed25519 shall be used as underlying cryptographic primitive.

If a key should be used in more than one primitive e.g. KeyExchange and AES-Encrypt-CBC, the CryptoKeyType could be extended by needed elements:

CryptoKeyType\_KeyExchange\_Cipher\_combined

- CryptoKeyElement\_KeyExchange\_Algorithm\_Ed25519
- CryptoKeyElement\_KeyExchange\_PartnerPubKey
- CryptoKeyElement\_KeyExchange\_OwnPubKey
- CryptoKeyElement\_KeyExchange\_Base
- CryptoKeyElement\_KeyExchange\_PrivKey
- CryptoKeyElement\_KeyExchange\_SharedValue
  - o ID = 1
- CryptoKeyElement\_Cipher\_IV

Note that CryptoKeyElement\_KeyExchange\_SharedValue has the id set to 1. When calling the encrypt service with a key of CryptoKeyType\_Cipher\_combined, the shared value of the key exchange is automatically used as encryption key.

## 7.2 General Behavior

The Crypto Driver can have one or more Crypto Driver Objects.

**[SWS\_Crypto\_00012]** [ In case several Crypto Driver instances (of same or different vendor) are implemented in one ECU the file names, API names, and published parameters must be distinguished such that no two definitions with the same name are generated.

The name shall be formatted according to **SWS\_BSW\_00102**: Crypto\_<vi>\_<ai>, where <vi> is the vendorId and <ai> is the vendorApiInfix.

]()

**[SWS\_Crypto\_00013]** [ The Crypto Driver may support all crypto primitives that are supported by the underlying hardware object.

] (SRS\_CryptoStack\_00098)

A job, declared in CSM specification [5], is an instance of a configured cryptographic primitive.

**[SWS\_Crypto\_00014]** [ A Crypto Driver Object shall only support processing one job at one time.

]()

**[SWS\_Crypto\_00117]** [ A Crypto Driver with n Crypto Driver Objects shall be able to process n jobs in parallel.

]()

Hint: Jobs, that are in the job queue (described in chapter 7.2.3.1), do not count as in processing.

### 7.2.1 Normal Operation

**[SWS\_Crypto\_00017]** [

“START” indicates a new request of a crypto primitive, and it shall cancel all previous requests of the same job.

]()

Note:

“job is being processed” means that the corresponding crypto driver object is currently and actively processing this job. When a job is not finished but the crypto driver object is not active with it (because, e.g., the operation “FINISH” is outstanding) this does not mean that this job is being processed.

Note:

To unite a single call function and a streaming approach for the crypto services, there is one interface `Crypto_ProcessJob()` with a service operation parameter (embedded in job structure parameter). This service operation is a flag field, that indicates the operation modes “START”, “UPDATE” or “FINISH”. It declares explicitly which operation will be performed.

If the “UPDATE” flag is set, the crypto primitive expects input data. “FINISH” indicates, that after this function call, all data are fed completely and the crypto primitive can finalize the calculations.

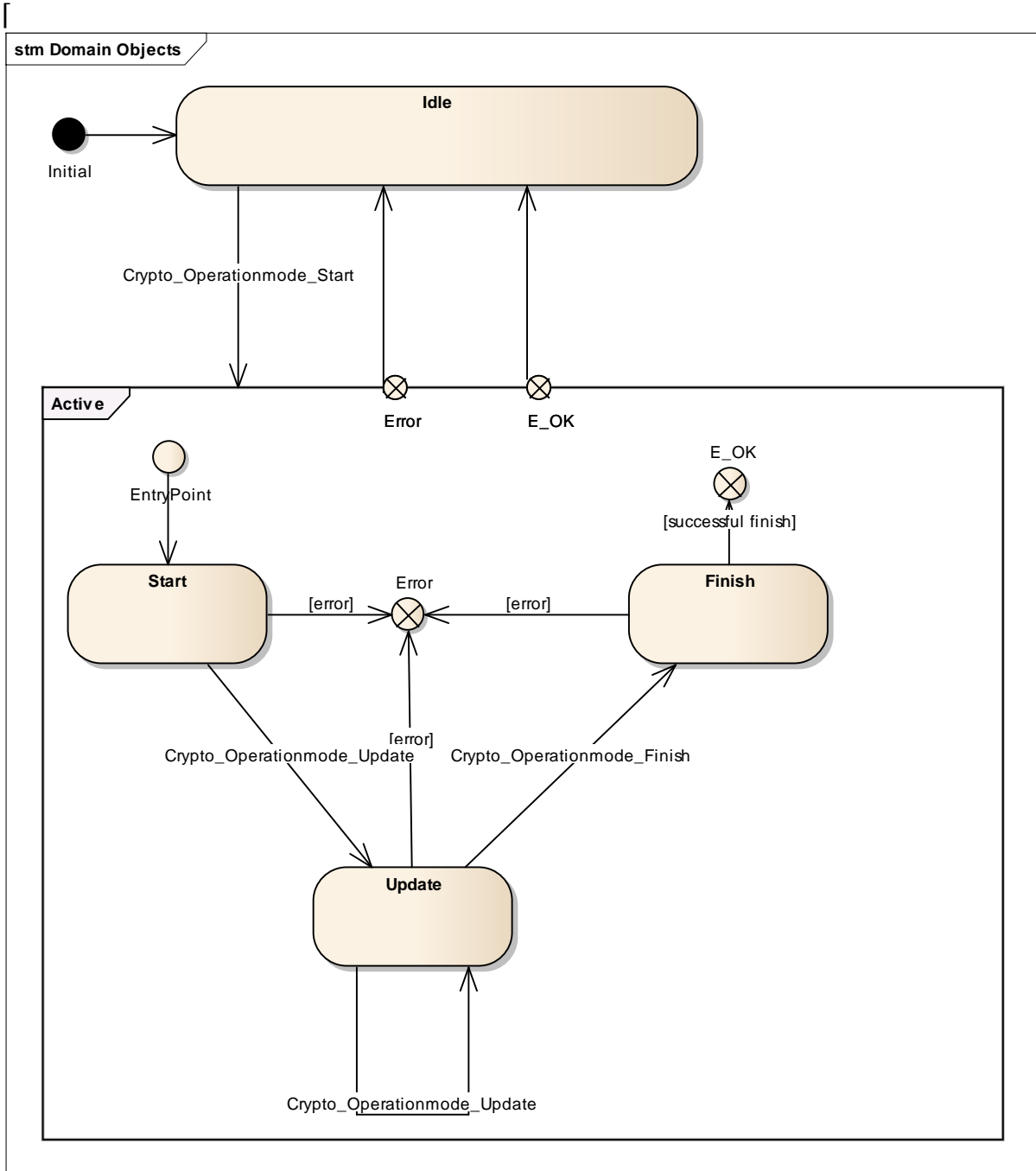
These operations can be combined to execute multiple operations at once. Then, the operations are performed in the order “START”, “UPDATE”, “FINISH”.



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

The diagram in SWS\_Crypto\_00018 shows the state machine of a job of this design without considering the transitions because of errors.

**[SWS\_Crypto\_00018]**



10)

**[SWS\_Crypto\_00019]** [ After initialization the crypto driver is in “idle” state.

]()

**[SWS\_Crypto\_00020]** [ If `Crypto_ProcessJob()` is called while in “Idle” or “Active” state and with the operation mode “START”, the previous request shall be cancelled. That means, that all previously buffered data for this job shall be reset, and the job shall switch to “Active” state and process the new one.

]()

Note:

Resetting a job using “START” is only possible when the job is not actively being processed.

**[SWS\_Crypto\_00118]** [ If `Crypto_ProcessJob()` is called while the job is in state “Idle” and the “START” flag in the operation mode is not set, the function shall return with `E_NOT_OK`.

]()

Note:

If `Crypto_ProcessJob()` is called while in “Active” state and with the operation mode “UPDATE”, the crypto primitive is fed with input data. In terms of streaming of arbitrary amounts of user data multiple calls with operation mode “UPDATE” is used, to feed more input data to the previously ones. In the “Update” state, there are usually also calculations of intermediate results of cryptographic primitives. Actually, in some cases (e.g. AES Encryption in CBC mode) there is also the generation of output data. While operating with the streaming approach (“Start”, “Update”, “Finish”) the Crypto Driver Object is waiting for further input (“Update”) until the “Finish” state has been reached. No other job could be processed meanwhile.

**[SWS\_Crypto\_00023]** [ If `Crypto_ProcessJob()` is called while in “Active” state and with the operation mode “FINISH”, the cryptographic calculations shall be finalized. Additional data (i.e. the MAC to be tested on a MAC verification service) shall be available at this point to process this job successfully. The results of the calculations shall be stored in the output buffers. At end of the processing the Crypto Driver shall switch to “Idle” state.

]()

To process a crypto service with a single call with `Crypto_ProcessJob()` the operation mode “`CRYPTO_OPERATIONMODE_SINGLECALL`” is a disjunction (bitwise OR) of the 3 modes “START”, “UPDATE” and “FINISH”.

**[SWS\_Crypto\_00025]** [ If an internal error occurs, the corresponding job state shall be set to “Idle” and all input data and intermediate results shall be discarded.

]()

**[SWS\_Crypto\_00119]** [ If an internal error occurs while processing an asynchronous job, the corresponding job state shall be set to “Idle” and all input data and intermediate results shall be discarded. Further, the callback notification shall be called with an appropriate error code.

l()

## 7.2.2 Functional Requirements

Note: The information whether the job shall be processed synchronously or asynchronously is part of the `Crypto_JobType`.

### 7.2.2.1 Synchronous Job Processing

**[SWS\_Crypto\_00026]** [ When the synchronous job processing is used, the corresponding interface functions shall compute the result synchronously within the context of this function call.

l()

**[SWS\_Crypto\_00199]** [ If the Crypto Driver has a queue and if a synchronous job is issued and the priority is greater than the highest priority available in the queue, the Crypto Driver shall disable processing new jobs from the queue until the next call of the main function has finished that follows after completion of the currently processed job.

l()

Note: Channels may hold jobs of both asynchronous and synchronous processing type. If so, a synchronous job might not be accepted for processing although its job's priority is higher than those of all asynchronous jobs.

### 7.2.2.2 Asynchronous Job Processing

**[SWS\_Crypto\_00027]** [ If the asynchronous job processing is used, the interface functions shall only hand over the necessary information to the primitive. The actual computation may be kicked-off by the main function.

l()

**[SWS\_Crypto\_00028]** [ For each asynchronous request the Crypto Driver shall notify CRYIF about the completion of the job by calling the `CRYIF_CallbackNotification` function passing on the job information and the result of cryptographic operation.

l()

## 7.2.3 Design Notes

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

### 7.2.3.1 Priority-dependent Job Queue

**[SWS\_Crypto\_00029]** [ Optionally, every Crypto Driver Object shall be able to line up jobs into a queue to process them one after the other.

l()

**[SWS\_Crypto\_00179]** [ The Crypto Driver Object shall disable queueing when the size of the crypto driver queue is set to 0.

]()

**[SWS\_Crypto\_00030]** [ The queue shall sort the jobs according to the configured jobs' priority.

]()

The higher the job priority value, the higher the job's priority.

**[SWS\_Crypto\_00031]** [ If `Crypto_ProcessJob()` is called, when the queue is empty and the Crypto Driver Object is not busy the Job shall switch to the state 'active' and execute the crypto primitive.

]()

**[SWS\_Crypto\_00032]** [ If `Crypto_ProcessJob()` is called and the queue is full, the function shall return with `CRYPTO_E_QUEUE_FULL`.

]()

Note:

It has to be ensured, that the asynchronous jobs are processed fast enough to avoid that the synchronous job has to wait for a long time.

It is also recommended to use `CRYPTO_OPERATIONMODE_SINGLECALL` for the asynchronous jobs.

Note:

A Crypto Driver Object can handle different jobs with synchronous and asynchronous job processing at the same time. However, synchronous job processing and job-queuing might not be useful. So, if synchronous job processing is chosen, the job queue will not be used, and a job will only be processed, when the Crypto Driver Object is not busy.

**[SWS\_Crypto\_00121]** [ If `Crypto_ProcessJob()` is called and the Job is in "ACTIVE" state, the `Crypto_ProcessJob()` shall check if the requested job matches the current job in the Crypto Driver Object and if yes, bypass it from queueing.

]()

This implicates that only jobs with operation mode „START“ shall be queued. If a job with operation mode "START" has been finished, the Crypto Driver Object is waiting for input. The callback function indicates the callee that an "UPDATE" or "FINISH" call shall be performed.

**[SWS\_Crypto\_00033]** [ If `Crypto_ProcessJob()` is called with asynchronous job processing and the queue is not full, but the Crypto Driver Object is busy and if the job has the operation mode "START", the Crypto Driver Object shall put the job into the queue and return `E_OK`.

]()

**[SWS\_Crypto\_00034]** [ If `Crypto_ProcessJob()` is called with synchronous job processing and the queue is not full, but the Crypto Driver Object is busy, the Crypto Driver Object shall not queue the job and return `CRYPTO_E_BUSY`. No job shall be put in any queue.

]()

## 7.2.4 Key Management

A key consists of one or more key elements.

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

Each key element has a defined access right for read or write access. The access right itself is defined by enumerations with an assigned value (see [\[ECUC\\_Crypto\\_00024\]](#) or [\[ECUC\\_Crypto\\_00027\]](#)) in the configuration of a `CryptoKeyElement`. The integer values of these enumerations are chosen in a way, that the assignment of an access right to a key element also deduces further right accesses. The lower the value, the higher the access right. This allows an easy compare of the assigned value to a required right access by numbers.

Example:

If a key element has access rights of `CRYPTO_RA_INTERNAL_COPY=2`, the right permission also applies to `CRYPTO_RA_ENCRYPTED=1` and `CRYPTO_RA_ALLOWED=0`, because both rights of the assigned enumeration values are lower and therefore are lower in the ranking of the access rights.

**[SWS\_Crypto\_00219]** [ Access rights shall be taken into account when direct access to key elements are required. This applies for read and write access.

]()

Keys or key elements can be copied using the key copy interface functions. This allows, for example, to store keys in one driver channel that provides secure key storage and to distribute them to other driver implementations that have no such capabilities. However, it is important that access rights to key elements are guarded within the copy operation to avoid unintended disclosure of stored keys.

**[SWS\_Crypto\_00220]** [ A source key element must have higher or the same rights than the destination key element when key elements are copied using the key copying interfaces. A source key must have at least the rights `CRYPTO_RA_INTERNAL_COPY` or lower to get copied.

]()

Info: An internal copy operation can only be performed if the key elements are located in the same crypto driver object.

**[SWS\_Crypto\_00221]** [ Jobs shall use the assigned key elements without guarding the key access rights with the following exceptions:

- If a key element is used for input using the input re-direction, the key element must have access rights `CRYPTO_RA_INTERNAL_COPY` or lower.

If input re-direction is used for CryptoPrimitiveService ENCRYPT/DECRYPT or AEAD\_ENCRYPT/AEAD\_DECRYPT, the access rights must be set to RA\_ENCRYPTED or lower.<sup>1)</sup>

- If a key element is used for output re-direction, the key element must have access rights CRYPTO\_WA\_INTERNAL\_COPY or lower.
- Any key element that is used to generate keys using Key Exchange operation shall have access rights of at least CRYPTO\_RA\_INTERNAL\_COPY or lower.
- For Key Derivation, the source key shall have access rights of at least CRYPTO\_RA\_INTERNAL\_COPY or lower. The destination key shall have at least the access right of its source key or lower<sup>2)</sup>.

] ()

<sup>1)</sup> Rationale: This is to avoid using a key element as input and (another for) output for encrypt and successively decrypt that key which would allow to extract the secret key in plaintext at the end.

<sup>2)</sup> This is to avoid to deduce the source key when using weak key derivation algorithms.

**[SWS\_Crypto\_00037]** [ The index of the different key elements from the different crypto services are defined as in imported types table SWS\_Csm\_01022.

]()

**[SWS\_Crypto\_00038]** [ A key has a state which is either “valid” or “invalid”.

]()

**[SWS\_Crypto\_00039]** [ If a key is in the state “invalid”, crypto services which make use of that key, shall return with CRYPTO\_E\_KEY\_NOT\_VALID.

]()

If a key (or key element) is currently in use by a crypto service, the state of the key has to be “valid”. When the `KeyElementSet()` is called, the key state is set to “invalid”. So, the job which is currently running will probably work with an inconsistent key. It is up to the application to only change key, if currently no primitive works with that key (element).

Note: The mapping of keys and key elements to SHE hardware functionality is possible without being subject to any restrictions except that read and write access through key management interfaces must be performed in encrypted form due to hardware constrains. To provide an environment for legacy software the single key used by the hardware can be placed in a key element referenced by several keys. Every key has also a unique reference to a key element containing an identifier. The driver implemented according to this specification can hence wrap existing SHE hard- and software and pass the data from the key elements to the existing SHE driver. In this use case one key element could contain a counter that could be read and written by the driver as well as the application. This counter could be used to detect if the key was overwritten. The loading of a key into the actual hardware key

slot could be done immediately before the key is used, which would result in a combined loading and processing of the key, as well as a separate operation following the writing of a key into a key element. This would result in separate operations for loading and processing the key.

If a new driver is to be implemented, it would also be possible to configure keys with completely independent key elements. These independent keys can be stored in RAM and passed to the hardware key slot only when required for an operation. The number of keys stored in the driver can be independent of (and much larger than) the number of hardware key slots. This requires, of course, a handling and storing of keys in software with all potential drawbacks.

Storing keys permanently is done by calling `Crypto_KeySetValid` with the configuration parameter `CryptoKeyElementPersist` set. As in most cases writing operation takes some time it is recommended to store key permanently using the `CRYPTO_KEYSETVALID` job interface.

Different key types can have compatible key elements. In this case the `keyElementId` has the same value. Key elements with the same `keyElementId` may be regarded as compatible. This way, the same key can be used for different services.

The key material therefore shall always have the `keyElementId` 1.

Example is the generation of a key with the Key Management Interface and usage of the same key in a primitive like `MacGenerate` afterwards.

**A key element may not be fully written. In some cases, the size of data to be stored in the key element can vary, e.g. asymmetric key elements. The Crypto Driver shall store the actually written size of data for internal usage and for exporting the element with `Crypto_KeyElementGet()`. If the key element shall allow to be not fully read or written can be configured with the parameter `CryptoKeyElementAllowPartialAccess` in the `CryptoKeyElement` container.**

## 7.2.5 Key Formats

**[SWS\_Crypto\_00184]** Asymmetric key material with identification is specified in accordance to RFC5958 in ASN.1 format. The key material with the format specifier `CRYPTO_KE_FORMAT_BIN_IDENT_PRIVATEKEY_PKCS8` needs to follow this format specification:

```
OneAsymmetricKey ::= SEQUENCE {
    version          Version,
    KeyAlgorithm     KeyAlgorithmIdentifier,
    keyMaterial      KeyMaterial,
    attributes*     [0] Attributes OPTIONAL,
    ...,
    [[2: publicKey* [1] PublicKey OPTIONAL ]],
    ...
}
```

\* The optional values for key attributes and the `PublicKey` are currently not used within the crypto driver and is listed here just for compatibility reason to RFC5958. A



driver shall tolerate the provision of this information but doesn't need to evaluate its contents.

The elements have the following meaning:

Version ::= INTEGER { v1(0), v2(1) } (v1, ..., v2)

KeyAlgorithmIdentifier ::= AlgorithmIdentifier  
                                   { PUBLIC-KEY,  
                                   { PrivateKeyAlgorithms } }

KeyMaterial ::= OCTET STRING

-- Content varies based on the type of the key and is specified by its

AlgorithmIdentifier.

-- The KeyAlgorithmIdentifier defines which format specifier for KeyMaterial shall be applied.

AlgorithmIdentifier: A value that identifies the format by its object identifier (OID).

] (SRS\_CryptoStack\_00008)

### 7.2.5.1 Definition of RSA Key Material

**[SWS\_Crypto\_00185]** For CRYPTO\_KE\_FORMAT\_BIN\_RSA\_PRIVATEKEY the parameter 'KeyMaterial OCTET STRING' for RSA private keys is defined according to IETF RFC8017 and has the following contents:

KeyMaterial ::= RSAPrivateKey

```
RSAPrivateKey ::= SEQUENCE {
  version Version,
  modulus INTEGER, -- n
  publicExponent INTEGER, -- e
  privateExponent INTEGER, -- d
  prime1 INTEGER, -- p
  prime2 INTEGER, -- q
  exponent1 INTEGER, -- d mod (p-1)
  exponent2 INTEGER, -- d mod (q-1)
  coefficient INTEGER -- (inverse of q) mod p }
```

Version ::= INTEGER { two-prime(0), multi(1) }

The fields of type RSAPrivateKey have the following meanings:

- version is the version number, for compatibility with future revisions of this document. It shall be 0 for this version of the document.
- modulus is the modulus n.
- publicExponent is the public exponent e.
- privateExponent is the private exponent d.
- prime1 is the prime factor p of n.
- prime2 is the prime factor q of n.
- exponent1 is d mod (p-1).
- exponent2 is d mod (q-1).
- coefficient is the Chinese Remainder Theorem coefficient (inverse of q) mod p.



] (SRS\_CryptoStack\_00008)

Note:

The values for prime1, prime2, exponent1, exponent2 and coefficient are optional. If prime1 is not provided, none of the following values in the list shall be provided. Otherwise, the key shall be rejected.

**[SWS\_Crypto\_00186]** The RSA public key in the format CRYPTO\_KE\_FORMAT\_BIN\_RSA\_PUBLICKEY is provided as follows:

```
RSAPublicKey ::= SEQUENCE {
    modulus INTEGER, -- n
    publicExponent INTEGER, -- e
}
```

The fields of type RSAPublicKey have the following meanings:

- modulus is the modulus n.
- publicExponent is the public exponent e.

] (SRS\_CryptoStack\_00008)

**[SWS\_Crypto\_00187]** The RSA public key in the format CRYPTO\_KE\_FORMAT\_BIN\_IDENT\_RSA\_PUBLICKEY is provided as follows:

```
PublicKeyInfo ::= SEQUENCE {
    KeyAlgorithmIdentifier ::= AlgorithmIdentifier,
    publicKey ::= RSAPublicKey
}
```

Explanation:

Considering RFC5280, section 4.1, the SubjectPublicKeyInfo follows directly the definition described above. Thus, a key type of CRYPTO\_KE\_FORMAT\_BIN\_IDENT\_PUBLICKEY matches SubjectPublicKeyInfo and CRYPTO\_KE\_FORMAT\_BIN\_RSA\_PUBLICKEY matches the subjectPublicKey in this definition.

] (SRS\_CryptoStack\_00008)

**[SWS\_Crypto\_00188]** The algorithm identifier for RSA keys shall have the value 1.2.840.113549.1.1.1. This corresponds to the ASN.1 coded OID value “2A 86 48 86 F7 0D 01 01 01”. This OID shall be provided whenever an AlgorithmIdentifier for RSA is required. In other words, when a key has the format CRYPTO\_KE\_FORMAT\_BIN\_IDENT\_PRIVATEKEY\_PKCS8 or CRYPTO\_KE\_FORMAT\_BIN\_IDENT\_PUBLICKEY and is used for RSA, the AlgorithmIdentifier must have this value.

Note: In some cases, a NULL value is followed directly to the OID. So, a value that follows directly after this OID in the same sequence is optional and should be tolerated.

] (SRS\_CryptoStack\_00008)

### 7.2.5.2 Definition of ECC Key Material

**[SWS\_Crypto\_00189]** Due to a lack of clear and efficient standard definition for ECC keys, key material for ECC is defined as binary information in the format definition of CRYPTO\_KE\_FORMAT\_BIN\_OCTET. The length of data depends on the assigned curve operation.

└ (SRS\_CryptoStack\_00008)

**[SWS\_Crypto\_00190]** Public keys for NIST and Brainpool ECC curves are provided with their X and Y coordinates:

ECC Public Key = Point X | Point Y.

The points are stored in little endian format.

The number of bytes for the key depends on the implementation of the curve.

Examples:

NIST curve P(256) public key = X(32) | Y(32)

NIST curve P(192) public key = X(24) | Y(24)

└ (SRS\_CryptoStack\_00008)

**[SWS\_Crypto\_00191]** Private keys for NIST and Brainpool ECC curves are provided with their X and Y coordinates and an additional scalar:

ECC Private Key = Point X | Point Y | Scalar.

The points and the scalar are stored in little endian format.

Example:

Brainpool curve P(256) = X(32) | Y(32) | SCALAR(32)

└ (SRS\_CryptoStack\_00008)

**[SWS\_Crypto\_00192]** The public key information for ED25519 contains a point on the curve:

ED25519 Public Key = Point X

The point is stored in little endian format.

Example:

ED25519 Public Key = X(32).

└ (SRS\_CryptoStack\_00008)

**[SWS\_Crypto\_00193]** The private key information for ED25519 contains a random constant and the point X on the curve:

ED25519 Private Key = Seed K | Point X

The point and the seed are stored in little endian format.

Example:

ED25519 Private Key = Seed K(32) | X(32).

└ (SRS\_CryptoStack\_00008)

## 7.3 Error classification

### 7.3.1 Development Errors

[SWS\_Crypto\_00040][

<i>Type of error</i>	<i>Related error code</i>	<i>Error value</i>
API request called before initialization of Crypto Driver.	CRYPTO_E_UNINIT	0x00
Initialization of Crypto Driver failed	CRYPTO_E_INIT_FAILED	0x01
API request called with invalid parameter (Nullpointer without redirection).	CRYPTO_E_PARAM_POINTER	0x02
API request called with invalid parameter (out of range).	CRYPTO_E_PARAM_HANDLE	0x04
API request called with invalid parameter (invalid value).	CRYPTO_E_PARAM_VALUE	0x05
Buffer is too small for operation	CRYPTO_E_SMALL_BUFFER	0x06

](SRS\_CryptoStack\_00086)

### 7.3.2 Runtime Errors

[SWS\_Crypto\_00194][

<i>Type of error</i>	<i>Related error code</i>	<i>Error value</i>
Requested key is not available	CRYPTO_E_RE_KEY_NOT_AVAILABLE	0x01
Key cannot be read	CRYPTO_E_RE_KEY_READ_FAIL	0x02
Entropy is too low	CRYPTO_E_RE_ENTROPY_EXHAUSTED	0x03

]()

### 7.3.3 Transient Faults

There are no transient faults.

### 7.3.4 Production Errors

There are no production errors.

### 7.3.5 Extended Production Errors

There are no production errors.

## 7.4 Error detection

**[SWS\_Crypto\_00217]** The crypto Driver shall check if job->cryptoKeyId and, if applicable, job->targetCryptoKeyId are in range, before it executes a job. If the check fails, the function Crypto\_ProcessJob shall report CRYPTO\_E\_PARAM\_HANDLE to DET and return E\_NOT\_OK.

!()

**[SWS\_Crypto\_00195]** If a Crypto Driver API is called and any buffer addressed during the operation is too small, then the operation shall not be performed. If development error detection for the Crypto Driver is enabled, then the API function shall report CRYPTO\_E\_SMALL\_BUFFER to the DET, else return E\_NOT\_OK.

!()

## 8 API specification

### 8.1 Imported types

In this chapter all types included from the following modules are listed:

#### [SWS\_Crypto\_00042]

<i>Module</i>	<i>Header File</i>	<i>Imported Type</i>
Csm	Crypto_GeneralTypes.h	Crypto_AlgorithmFamilyType
	Crypto_GeneralTypes.h	Crypto_AlgorithmInfoType
	Crypto_GeneralTypes.h	Crypto_AlgorithmModeType
	Crypto_GeneralTypes.h	Crypto_JobInfoType
	Crypto_GeneralTypes.h	Crypto_JobPrimitiveInfoType
	Crypto_GeneralTypes.h	Crypto_JobPrimitiveInputOutputType
	Crypto_GeneralTypes.h	Crypto_JobRedirectionInfoType
	Crypto_GeneralTypes.h	Crypto_JobStateType
	Crypto_GeneralTypes.h	Crypto_JobType
	Crypto_GeneralTypes.h	Crypto_PrimitiveInfoType
	Crypto_GeneralTypes.h	Crypto_ProcessingType
	Crypto_GeneralTypes.h	Crypto_ServiceInfoType
	Rte_Csm_Type.h	Crypto_OperationModeType
	Rte_Csm_Type.h	Crypto_VerifyResultType
Std	Std_Types.h	Std_ReturnType
	Std_Types.h	Std_VersionInfoType

l()

In addition to the imported types listed in SWS\_Crypto\_00042, the following type is also required and need to be imported by the Crypto Driver:

<b>Module</b>	<b>Header File</b>	<b>Imported Type</b>
Csm	Crypto_GeneralTypes.h	Crypto_ReturnType

The Crypto Stack API uses this type as an extension to Std\_ReturnType to return additional error codes within the crypto stack (see also SWS\_Csm\_91043 for reference).

Note:

CRYPTO\_E\_KEY\_NOT\_AVAILABLE is meant to indicate that the key has been programmed before but cannot be accessed at the moment (for instance it is temporarily not accessible, e.g. when the key is disabled due to debugger connection or parameters are wrong).

CRYPTO\_E\_KEY\_EMPTY is meant to indicate that the referred key content has not been written so far and has no default value (For example, in SHE 1.1, the error code ERC\_KEY\_EMPTY would be returned then, "if the application attempts to use a key that has not been initialized".)

Furthermore, it should be noted, that the Crypto Stack API uses the key element index definition from the CSM module (see SWS\_Csm\_00122).

## 8.2 Type Definitions

### [SWS\_Crypto\_91016]

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

](SWS\_BSW\_00216)

## 8.3 Function definitions

This is a list of functions provided for upper layer modules.

### 8.3.1 General API

#### 8.3.1.1 Crypto\_Init

[SWS\_Crypto\_91000][

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

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

[SWS\_Crypto\_00215] [ The Configuration pointer `configPtr` shall always have a null pointer value.

] (SWS\_BSW\_00050)

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

[SWS\_Crypto\_00198][

If during initialization of the Crypto Driver the value of a persistent key could not be loaded, the Crypto Driver shall set the state of the corresponding key to invalid.

]()

Note: After initialization of the Crypto Driver and before the application starts, the application should consider to check the state of the configured keys and to implement an appropriate handling if the key's state is invalid.

[SWS\_Crypto\_00045] [ If the initialization of the Crypto Driver fails, the Crypto shall report `CRYPTO_E_INIT_FAILED` to the DET.

]()

#### 8.3.1.2 Crypto\_GetVersionInfo

[SWS\_Crypto\_91001][

<b>Service Name</b>	Crypto_GetVersionInfo
---------------------	-----------------------

<b>Syntax</b>	void Crypto_GetVersionInfo ( Std_VersionInfoType* versioninfo )	
<b>Service ID [hex]</b>	0x01	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant	
<b>Parameters (in)</b>	versioninfo	Pointer to where to store the version information of this module.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	void	--
<b>Description</b>	Returns the version information of this module.	
<b>Available via</b>	Crypto.h	

](SRS\_BSW\_00407)

**[SWS\_Crypto\_00047]** [ If the parameter `versioninfo` is a null pointer and if development error detection for the Crypto Driver is enabled, the function `Crypto_GetVersionInfo` shall report `CRYPTO_E_PARAM_POINTER` to the DET.  
]()

## 8.3.2 Job Processing Interface

### 8.3.2.1 Crypto\_ProcessJob

**[SWS\_Crypto\_91003]**[

<b>Service Name</b>	Crypto_ProcessJob	
<b>Syntax</b>	Std_ReturnType Crypto_ProcessJob ( uint32 objectId, Crypto_JobType* job )	
<b>Service ID [hex]</b>	0x03	
<b>Sync/Async</b>	Asynchronous or Async, depends on the job configuration	
<b>Reentrancy</b>	Reentrant	
<b>Parameters (in)</b>	objectId	Holds the identifier of the Crypto Driver Object.
<b>Parameters (inout)</b>	job	Pointer to the configuration of the job. Contains structures with job and primitive relevant information but also pointer to result buffers.
<b>Parameters (out)</b>	None	



<p><b>Return value</b></p>	<p>Std_- Return- Type</p>	<p>E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy CRYPTO_E_KEY_NOT_VALID: Request failed, the key is not valid CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, a key element has the wrong size CRYPTO_E_QUEUE_FULL: Request failed, the queue is full CRYPTO_E_KEY_READ_FAIL: The service request failed, because key element extraction is not allowed CRYPTO_E_KEY_WRITE_FAIL: The service request failed because the writing access failed CRYPTO_E_KEY_NOT_AVAILABLE: The service request failed because the key is not available CRYPTO_E_ENTROPY_EXHAUSTED: Request failed, the entropy is exhausted CRYPTO_E_JOB_CANCELED: The service request failed because the synchronous Job has been canceled CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element</p>
<p><b>Description</b></p>	<p>Performs the crypto primitive, that is configured in the job parameter.</p>	
<p><b>Available via</b></p>	<p>Crypto.h</p>	

l()

This Interface has a different behavior depending on the content of the `job` parameter (i.e. the type of crypto service).

Depending on this configuration, other input parameters within the `job` need to be set, in order to call this function successfully. I.e. the MAC Generate crypto primitive requires a key, a plaintext to be used, and a buffer for the generated MAC.

**[SWS\_Crypto\_00057]** [ If the module is not initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_ProcessJob` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00058]** [ If the parameter `objectId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_ProcessJob` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00059]** [ If the parameter `job` is a null pointer and if development error detection for the Crypto Driver is enabled, the function `Crypto_ProcessJob` shall report `CRYPTO_E_PARAM_POINTER` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00064]** [ If the parameter `job->jobPrimitiveInfo->primitiveInfo->service` is not supported by the Crypto Driver Object and

if development error detection for the Crypto Driver is enabled, the function `Crypto_ProcessJob` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`  
|() )

**[SWS\_Crypto\_00201]**

If the parameter `job->jobPrimitiveInfo->primitiveInfo->service` is set to `CRYPTO_KEYSETVALID`, `CRYPTO_RANDOMSEED`, `CRYPTO_KEYGENERATE`, `CRYPTO_KEYDERIVE`, `CRYPTO_KEYEXCHANGEALCPUBVAL` or `CRYPTO_KEYEXCHANGEALCSECRET`, the parameter `job->cryptoKeyld` must be in range; else the function `Crypto_ProcessJob` shall report `CRYPTO_E_PARAM_HANDLE` to DET and return `E_NOT_OK`.  
|() )

**[SWS\_Crypto\_00202]**

If the parameter `job->jobPrimitiveInfo->primitiveInfo->service` is set to `CRYPTO_KEYDERIVE`, the parameter `job->cryptoTargetKeyld` must be in range; else the function `Crypto_ProcessJob` shall report `CRYPTO_E_PARAM_HANDLE` to DET and return `E_NOT_OK`  
|() )

**[SWS\_Crypto\_00065]** [ If `job->jobPrimitiveInfo->primitiveInfo->service` is set to `CRYPTO_HASH` or `CRYPTO_MACGENERATE`, the parameter `job->jobPrimitiveInfo->primitiveInfo->resultLength` is required. If the configured result length of the job is smaller than the result length of the chosen algorithm, the most significant bits of the result shall be truncated to the configured result length.  
|() )

**[SWS\_Crypto\_00067]** [

If the parameter `job->jobPrimitiveInfo->primitiveInfo->algorithm` (with its variation in `family`, `keyLength` and `mode`) is not supported by the Crypto Driver Object and if development error detection for the Crypto Driver is enabled, the function `Crypto_ProcessJob` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.  
|() )

Depending of the crypto service configured in `job->jobPrimitiveInfo->primitiveInfo->service`, different parameters of `job->jobPrimitiveInput` are required to be set with valid values. The table in `SWS_Crypto_00071` specifies which parameters are required or optional for a service in different modes. The following requirements specify the behavior if a required member is a null pointer.

**[SWS\_Crypto\_00070]** [

If a pointer to a buffer is required as an argument, but it is a null pointer, the `Crypto_ProcessJob()` function shall report `CRYPTO_E_PARAM_POINTER` to the DET if development error detection for the Crypto Driver is enabled, and return `E_NOT_OK`.

]()

**[SWS\_Crypto\_00142] [**

If a length information is required for processing a service request, either as variable or pointer, but the indicated length value is zero, and if development error detection for the Crypto Driver is enabled, the `Crypto_ProcessJob()` function report `CRYPTO_E_PARAM_VALUE` to the DET and return `E_NOT_OK`.

]()

**[SWS\_Crypto\_00071] [**

Member  Service*	inputPtr / **redirected input	inputLength	secondaryInputPtr / **redirected input	secondaryInputLength	tertiaryInputPtr / **redirected input	tertiaryInputLength	outputPtr / ***redirected output	outputLengthPtr	secondaryOutputPtr/ ***redirected output	secondaryOutputLengthPtr	verifyPtr	mode
HASH	UG	UG					F	F				SUF
MACGENERATE	UG	UG					F	F				SUF
MACVERIFY	UG	UG	F	F							F	SUF
ENCRYPT	UG	UG					UF	UF				SUF
DECRYPT	UG	UG					UF	UF				SUF
AADENCRYPT	UG	UG	F	F			UF	UF	F	F		SUF
AADDECRYPT	UG	UG	F	F	F	F	UF	UF			F	SUF
SIGNATUREGENERATE	UG	UG					F	F				SUF
SIGNATUREVERIFY	UG	UG	F	F							F	SUF
RANDOMGENERATE							F	F				

\*: Service names are derived from `Crypto_ServiceInfoType` (part of job struct)

\*\* : In case of input redirection the corresponding key element is used as input instead of the `inputBuffer`.

\*\*\*: In case of output redirection the corresponding key element is used as output instead of the `outputBuffer`

**S**: member required in Start mode.

**U**: member required in Update mode.

**F**: member required in Finish mode.

**G**: member optional in Finish mode.

]()

**[SWS\_Crypto\_00072]** [ All crypto services listed in `Crypto_ServiceInfoType` except of `CRYPTO_HASH`, and `CRYPTO_RANDOMGENERATE` require a key represented as a key identifier .

]()

**[SWS\_Crypto\_00073]** [ In the following table the content of the different input and output buffers of `job.jobPrimitiveInputOutputType` are specified:

<b>Service*</b>	<b>Parameter</b>	Input**	Secondary Input**	Tertiary Input**	Output***	Secondary Output***	Crylf KeyId	Target Crylf KeyId
HASH		plaintext			generated hash			
MACGENERATE		plaintext			generated MAC			
MACVERIFY		plaintext	MAC to be verified					
ENCRYPT		plaintext			encrypted ciphertext			
DECRYPT		ciphertext			decrypted plaintext			
AADENCRYPT		plaintext	associated Data		encrypted ciphertext	generated Tag		
AADDECRYPT		ciphertext	associated Data	Tag to be verified	decrypted Plaintext			
SIGNATUREGENERATE		plaintext			generated signature			
SIGNATUREVERIFY		plaintext	signature to be verified					
RANDOMGENERATE					Generated random			
RANDOMSEED		Seed					KeyId	Target KeyId
KEYGENERATE							KeyId	
KEYDERIVE							KeyId	Target KeyId
KEYEXCHANGE CALCPUBVAL			Public Value				KeyId	
KEYEXCHANGE CALCSECRET		Partner's Public Value					KeyId	
KEYSETVALID							KeyId	

\*: Service names are derived from `Crypto_ServiceInfoType`.

\*\* : In case of input redirection the corresponding key element is used as input instead of the `inputBuffer`.

\*\*\* : In case of output redirection the corresponding key element is used as output instead of the `output buffer`

]()

If no errors are detected by the Crypto Driver, the Crypto Driver processes the crypto service, configured in `job`, with the underlying hardware or software solutions.

**[SWS\_Crypto\_00134]** [ If the crypto primitive requires input data, its memory location is referred by the pointer `job->jobPrimitiveInput.inputPtr`. On calling `Crypto_ProcessJob`, the length of this data is stored in `job->jobPrimitiveInput.inputLength`.

This applies analogously to `job->jobPrimitiveInput.secondaryInputPtr` and `job->jobPrimitiveInput.secondaryInputLength` respectively `job->jobPrimitiveInput.tertiaryinputPtr` and `job->jobPrimitiveInput.tertiaryInputLength`, if they shall be used for the chosen crypto primitive.

If the input is redirected to a key element, the input buffer of the respective key element has to be used.

()

**[SWS\_Crypto\_00203]** [ If `job->jobRedirectionInfoRef` is not a `NULLPTR` and the configuration bit for the `inputRedirection`, `secondaryInputRedirection` and/or `tertiaryInputRedirection` is set within `job->jobRedirectionInfoRef->redirectionConfig`, then the corresponding key element buffer located by `job->jobRedirectionInfoRef->inputKeyId+ job->jobRedirectionInfoRef->inputKeyElementId`, `job->jobRedirectionInfoRef->secondaryInputKeyId+ job->jobRedirectionInfoRef->secondaryInputKeyElementId`, and/or `jobRedirectionInfoRef->tertiaryInputKeyId+ job->jobRedirectionInfoRef->tertiaryInputKeyElementId` and its length shall be used.

Any data provided by the input parameter of the function interface shall be ignored.

()

**[SWS\_Crypto\_00135]** [

If the crypto primitive requires a buffer for the result, its memory location is referred by the pointer `job->jobPrimitiveInput.outputPtr`. On calling this function, `job->jobPrimitiveInput.outputLengthPtr` shall contain the size of the associated buffer. When the request has finished, the actual length of the returned value shall be stored.

This applies analogously to `job->jobPrimitiveInput.secondaryOutputPtr` and `job->jobPrimitiveInput.secondaryOutputLengthPtr`, if they shall be used for the chosen crypto primitive.

If the output is redirected to a key element, the output buffer of the respective key element has to be used instead.

()

**[SWS\_Crypto\_00204]** [ If `job->jobRedirectionInfoRef` is not a `NULLPTR` and the configuration bit for the `outputRedirection` and/or `secondaryoutputRedirection` is set within `job-> jobRedirectionInfoRef->redirectionConfig`, then the corresponding key element buffer located by `job-> jobRedirectionInfoRef->outputKeyId + job-> jobRedirectionInfoRef->outputKeyElementId` and/or `job-> jobRedirectionInfoRef->secondaryOutputKeyId + job-> jobRedirectionInfoRef->secondaryOutputKeyElementId` shall be used as output. The length of the respective key element shall be set according to the length of the output.

]()

**[SWS\_Crypto\_00141]** [ If the random generator service is chosen and the corresponding entropy, the function shall return `CRYPTO_E_ENTROPY_EXHAUSTED`. The function `Crypto_ProcessJob` shall additionally report the runtime error `CRYPTO_E_RE_ENTROPY_EXHAUSTED`.

]()

### 8.3.3 Job Cancellation Interface

#### 8.3.3.1 Crypto\_CancelJob

**[SWS\_Crypto\_00122]**[

<b>Service Name</b>	Crypto_CancelJob	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_CancelJob (     uint32 objectId,     Crypto_JobType* job )</pre>	
<b>Service ID [hex]</b>	0x0e	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for same Crypto Driver Object	
<b>Parameters (in)</b>	objectId	Holds the identifier of the Crypto Driver Object.
<b>Parameters (inout)</b>	job	Pointer to the configuration of the job. Contains structures with job and primitive relevant information.
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_ReturnType	E_OK: Request successful, job has been removed. E_NOT_OK: Request failed, job couldn't be removed. CRYPTO_E_JOB_CANCELED: The job has been cancelled but is still processed. No results will be returned to the application.
<b>Description</b>	This interface removes the provided job from the queue and cancels the processing of the job if possible.	
<b>Available via</b>	Crypto.h	

]()

**[SWS\_Crypto\_00123]** [ If development error detection for the Crypto Driver is enabled: The function `Crypto_CancelJob` shall raise the error `CRYPTO_E_UNINIT` and return `E_NOT_OK` if the module is not yet initialized.

]()

**[SWS\_Crypto\_00124]** [ If development error detection for the Crypto Driver is enabled: The function `Crypto_CancelJob` shall raise the error `CRYPTO_E_PARAM_HANDLE` and return `E_NOT_OK` if the parameter `objectId` is out of range.

]()

**[SWS\_Crypto\_00125]** [ If development error detection for the Crypto Driver is enabled: The function `Crypto_CancelJob` shall raise the error `CRYPTO_E_PARAM_POINTER` and return `E_NOT_OK` if the parameter `job` is a null pointer.

]()

**[SWS\_Crypto\_00214]** [ If no errors are detected by Crypto Driver and the driver does currently not process this job, the service `Crypto_CancelJob()` shall return `E_OK` without any processing.

]()

**[SWS\_Crypto\_00143]** [ If no errors are detected by Crypto Driver and the driver is able to cancel the job immediately, the service `Crypto_CancelJob()` shall remove the job from the queue and cancel the job in the hardware. If the cancellation is successful `E_OK` shall be returned, otherwise it shall return `E_NOT_OK`.

]()

Note:

Especially hardware implementations may not support a cancelation. If `Crypto_CancelJob()` is called and immediate cancelation is not possible at least all results and notifications of the job shall be suppressed. The caller can be sure, that there will be no (intermediate) results by callback or synchronous result value.

**[SWS\_Crypto\_00183]** [ If no errors are detected by Crypto Driver and the driver is not able to cancel the job (e.g. due to hardware limitations), the service `Crypto_CancelJob()` shall return `CRYPTO_E_JOB_CANCELED`.

]()

Note:

`SWS_Crypto_00183` should not have any effect on the job processing in the Crypto Driver. The processing should be completed as any other regular job. The CSM guarantees that the result buffer pointer is valid until the job is finished.



### 8.3.4 Key Management Interface

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

**[SWS\_Crypto\_00145]** [ If the underlying crypto hardware does not allow execution of key management functions at the same time as processing a job, the key management functions shall wait while the current job is executed and start the processing of the key management function afterwards.

]()

Note:

It has to be ensured, that the jobs are processed fast enough to avoid that the key management function has to wait for a long time.

It is also recommended to use CRYPTO\_OPERATIONMODE\_SINGLECALL for the jobs.

#### 8.3.4.1 Key Setting Interface

##### 8.3.4.1.1 Crypto\_KeyElementSet

**[SWS\_Crypto\_00223]** [ The crypto driver shall only perform this operation if `CryptoKeyElement/CryptoKeyElementWriteAccess` is set to `CRYPTO_WA_ALLOWED` or `CRYPTO_WA_ENCRYPTED`.

] ()

Note: If the key element references a SHE-key, it is recommended to set `CryptoKeyElementWriteAccess` to `CRYPTO_WA_ENCRYPTED`. The key itself must be provided as SHE-keys in the format M1M2M3.

**[SWS\_Crypto\_91004]**

<b>Service Name</b>	Crypto_KeyElementSet	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyElementSet (     uint32 cryptoKeyId,     uint32 keyElementId,     const uint8* keyPtr,     uint32 keyLength )</pre>	
<b>Service ID [hex]</b>	0x04	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Non Reentrant	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key whose key element shall be set.
	keyElementId	Holds the identifier of the key element which shall be set.



	keyPtr	Holds the pointer to the key data which shall be set as key element.
	keyLength	Contains the length of the key element in bytes.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_Return-Type	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy CRYPTO_E_KEY_WRITE_FAIL: Request failed because write access was denied CRYPTO_E_KEY_NOT_AVAILABLE: Request failed because the key is not available CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element size does not match size of provided data
<b>Description</b>	Sets the given key element bytes to the key identified by cryptoKeyId.	
<b>Available via</b>	Crypto.h	

l()

Note: This service works synchronously. However, it is possible that the underlying key material is resident in the flash memory. Hence it may take some time to execute this function.

**[SWS\_Crypto\_00075]** [ If the Crypto Driver is not yet initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementSet` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00076]** [ If `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementSet` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00077]** [ If parameter `keyElementId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementSet` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00078]** [ If the parameter `keyPtr` is a null pointer and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementSet` shall report `CRYPTO_E_PARAM_POINTER` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00079]** [ If `keyLength` is zero and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementSet` shall report `CRYPTO_E_PARAM_VALUE` to the DET and return `E_NOT_OK`.  
|() ]()

**[SWS\_Crypto\_00146]** [ If `keyLength` is smaller than the size of the key element, and the key element is not configured to allow partial access, the function `Crypto_KeyElementSet` shall return `CRYPTO_E_KEY_SIZE_MISMATCH`.  
|() ]()

### 8.3.4.1.2 Crypto\_KeySetValid

**[SWS\_Crypto\_91014]**[

<b>Service Name</b>	Crypto_KeySetValid	
<b>Syntax</b>	Std_ReturnType Crypto_KeySetValid ( uint32 cryptoKeyId )	
<b>Service ID [hex]</b>	0x05	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Non Reentrant	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key which shall be set to valid.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_Return-Type	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy
<b>Description</b>	Sets the key state of the key identified by <code>cryptoKeyId</code> to valid.	
<b>Available via</b>	Crypto.h	

|() ]()

**[SWS\_Crypto\_00196]** [ If the module is not yet initialized and development error detection for the Crypto Driver is enabled, the function `Crypto_KeySetValid` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.  
| () ] () ]()

**[SWS\_Crypto\_00197]** [ If parameter `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function

Crypto\_KeySetValid shall report CRYPTO\_E\_PARAM\_HANDLE to the DET and return E\_NOT\_OK.

] ()

If no errors are detected by Crypto Driver, the service Crypto\_KeySetValid() sets the key cryptoKeyId to “valid”.

### 8.3.4.2 Key Extraction Interface

#### 8.3.4.2.1 Crypto\_KeyElementGet

[SWS\_Crypto\_00222] [ The crypto driver shall only perform this operation if CryptoKeyElement/CryptoKeyElementReadAccess is set to CRYPTO\_RA\_ALLOWED or CRYPTO\_RA\_ENCRYPTED.

] ()

Note: Reading keys from SHE hardware is not possible, except if it is a SHE RAM-Key. In this case, reading the SHE key will provide M1M2M3. The key element should be set to CRYPTO\_RA\_ENCRYPTED in this case.

[SWS\_Crypto\_91006]

<b>Service Name</b>	Crypto_KeyElementGet	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyElementGet (     uint32 cryptoKeyId,     uint32 keyElementId,     uint8* resultPtr,     uint32* resultLengthPtr )</pre>	
<b>Service ID [hex]</b>	0x06	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key whose key element shall be returned.
	keyElementId	Holds the identifier of the key element which shall be returned.
<b>Parameters (inout)</b>	resultLengthPtr	Holds a pointer to a memory location in which the length information is stored. On calling this function this parameter shall contain the size of the buffer provided by resultPtr. If the key element is configured to allow partial access, this parameter contains the amount of data which should be read from the key element. The size may not be equal to the size of the provided buffer anymore. When the request has finished, the amount of data that has been stored shall be stored.
<b>Parameters (out)</b>	resultPtr	Holds the pointer of the buffer for the returned key element

<b>Return value</b>	Std_ - Return- Type	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy CRYPTO_E_KEY_NOT_AVAILABLE: Request failed, the requested key element is not available CRYPTO_E_KEY_READ_FAIL: Request failed because read access was denied CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element
<b>Description</b>	This interface shall be used to get a key element of the key identified by the crypto KeyId and store the key element in the memory location pointed by the result pointer. Note: If the actual key element is directly mapped to flash memory, there could be a bigger delay when calling this function (synchronous operation).	
<b>Available via</b>	Crypto.h	

l()

**[SWS\_Crypto\_00140]** | If the function `Crypto_KeyElementGet` returns `CRYPTO_E_KEY_NOT_AVAILABLE`, the function shall additionally report the runtime error `CRYPTO_E_RE_KEY_NOT_AVAILABLE`.

l()

**[SWS\_Crypto\_00139]** | If the function `Crypto_KeyElementGet` returns `CRYPTO_E_KEY_READ_FAIL`, the function shall additionally report the runtime error `CRYPTO_E_RE_KEY_READ_FAIL`.

l()

**[SWS\_Crypto\_00085]** | If the module is not yet initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementGet` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00086]** | If the parameter `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementGet` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00087]** | If the parameter `keyElementId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementGet` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00088]** | If the parameter `resultPtr` is a null pointer and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementGet` shall report `CRYPTO_E_PARAM_POINTER` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00089]** [ If the parameter `resultLengthPtr` is a null pointer and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementGet` shall report `CRYPTO_E_PARAM_POINTER` to the DET and return `E_NOT_OK`.

]()

**[SWS\_Crypto\_00090]** [ If the value, which is pointed by `resultLengthPtr` is zero and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementGet` shall report `CRYPTO_E_PARAM_VALUE` to the DET and return `E_NOT_OK`.

]()

If no errors are detected by Crypto Driver, the service `Crypto_KeyElementGet()` retrieves the value of the key element and store it in the buffer, which is pointed by the `resultPtr`.

**[SWS\_Crypto\_00092]** [ The pointer `resultPtr` holds the memory location, where the data of the key element shall be stored. On calling this function, `resultLengthPtr` shall contain the size of the buffer provided by `resultPtr`. When the request has finished, the actual length of the returned value shall be stored.

]()

### 8.3.4.3 Key Copying Interface

#### 8.3.4.3.1 `Crypto_KeyElementCopy`

**[SWS\_Crypto\_00148]**[

<b>Service Name</b>	<code>Crypto_KeyElementCopy</code>	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyElementCopy (     uint32 cryptoKeyId,     uint32 keyElementId,     uint32 targetCryptoKeyId,     uint32 targetKeyElementId )</pre>	
<b>Service ID [hex]</b>	0x0f	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for the same <code>cryptoKeyId</code>	
<b>Parameters (in)</b>	<code>cryptoKeyId</code>	Holds the identifier of the key whose key element shall be the source element.
	<code>keyElementId</code>	Holds the identifier of the key element which shall be the source for the copy operation.
	<code>targetCryptoKey</code>	Holds the identifier of the key whose key element shall be the

	Id	destination element.
	targetKey ElementId	Holds the identifier of the key element which shall be the destination for the copy operation.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_ReturnType	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy CRYPTO_E_KEY_NOT_AVAILABLE: Request failed, the requested key element is not available CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element
<b>Description</b>	Copies a key element to another key element in the same crypto driver. Note: If the actual key element is directly mapped to flash memory, there could be a bigger delay when calling this function (synchronous operation)	
<b>Available via</b>	Crypto.h	

l()

**[SWS\_Crypto\_00149]** [ If the Crypto Driver is not yet initialized and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyElementCopy` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00150]** [ If `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementCopy` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00151]** [ If `targetCryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyElementCopy` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00152]** [ If parameter `keyElementId` is out of range and if development error detection for the Crypto Driver is enabled, the function

Crypto\_KeyElementCopy shall report CRYPTO\_E\_PARAM\_HANDLE to the DET and return E\_NOT\_OK.

]()

**[SWS\_Crypto\_00153]** [ If parameter targetKeyId is out of range and if development error detection for the Crypto Driver is enabled, the function

Crypto\_KeyElementCopy shall report CRYPTO\_E\_PARAM\_HANDLE to the DET and return E\_NOT\_OK.

]()

**[SWS\_Crypto\_00154]** If no errors are detected by the Crypto Driver, the function shall copy the key element referenced by keyElementId in the key referenced by cryptoKeyId to the key element referenced by targetKeyId in the key referenced by targetCryptoKeyId.

### 8.3.4.3.2 Crypto\_KeyElementCopyPartial

**[SWS\_Crypto\_91015]**

<b>Service Name</b>	Crypto_KeyElementCopyPartial	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyElementCopyPartial (     uint32 cryptoKeyId,     uint32 keyElementId,     uint32 keyElementSourceOffset,     uint32 keyElementTargetOffset,     uint32 keyElementCopyLength,     uint32 targetCryptoKeyId,     uint32 targetKeyElementId )</pre>	
<b>Service ID [hex]</b>	0x13	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for the same cryptoKeyId	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key whose key element shall be the source element.
	keyElementId	Holds the identifier of the key element which shall be the source for the copy operation.
	keyElementSourceOffset	This is the offset of the of the source key element indicating the start index of the copy operation.
	keyElementTargetOffset	This is the offset of the of the target key element indicating the start index of the copy operation.
	keyElementCopyLength	Specifies the number of bytes that shall be copied.
	targetCryptoKeyId	Holds the identifier of the key whose key element shall be the destination element.

	targetKeyId	Holds the identifier of the key element which shall be the destination for the copy operation.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_ReturnType	<p>E_OK: Request successful  E_NOT_OK: Request failed  CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy  CRYPTO_E_KEY_NOT_AVAILABLE: Request failed, the requested key element is not available  CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element  CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element  CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible  CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element</p>
<b>Description</b>	<p>Copies a key element to another key element in the same crypto driver. The key ElementSourceOffset and keyElementCopyLength allows to copy just a part of the source key element into the destination. The offset of the target key is also specified with this function.  Note: If the actual key element is directly mapped to flash memory, there could be a bigger delay when calling this function (synchronous operation).</p>	
<b>Available via</b>	Crypto.h	

{}()

**[SWS\_Crypto\_00205]** [ If the Crypto Driver is not yet initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementCopyPartial` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

{}()

**[SWS\_Crypto\_00206]** [ If `cryptoKeyId`, `keyElementId`, `targetKeyId` or `targetCryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementCopyPartial` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

{}()

**[SWS\_Crypto\_00207]** [ If the total length of the key element specified with `keyElementId` of the key referenced by `cryptoKeyId` is smaller than `keyElementSourceOffset + keyElementCopyLength` `Crypto_KeyElementCopyPartial` shall return `CRYPTO_E_KEY_SIZE_MISMATCH`.

{}()



**[SWS\_Crypto\_00208]** [ If the maximum available buffer of the key element specified with `targetKeyElementId` of the key referenced by `targetCryptoKeyId` is smaller than `keyElementTargetOffset + keyElementCopyLength`, the function `Crypto_KeyElementCopyPartial` shall return `CRYPTO_E_KEY_SIZE_MISMATCH`.  
]()

**[SWS\_Crypto\_00209]** [ If no errors are detected by the Crypto Driver, the function `Crypto_KeyElementCopyPartial` shall copy a part of the key element referenced by `keyElementId` of the key referenced by `cryptoKeyId` with the offset of `keyElementSourceOffset` and with the length specified by `keyElementCopyLength` to the key element referenced by `targetKeyElementId` of the key referenced by `targetCryptoKeyId`.  
]()

**[SWS\_Crypto\_00210]** [ If the current length of the target key element is greater or equal than  $(keyElementTargetOffset + keyElementCopyLength)$ , the key element length remains unchanged.  
]()

**[SWS\_Crypto\_00211]** [ If the current length of the target key element is lower than  $(keyElementTargetOffset + keyElementCopyLength)$  and the maximum length of the key element is greater or equal than  $(keyElementTargetOffset + keyElementCopyLength)$ , then the source data shall be copied into the target key element and the length shall be set to  $(keyElementTargetOffset + keyElementCopyLength)$ .  
]()

### 8.3.4.3.3 Crypto\_KeyCopy

**[SWS\_Crypto\_00155]**[

<b>Service Name</b>	Crypto_KeyCopy	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyCopy (     uint32 cryptoKeyId,     uint32 targetCryptoKeyId )</pre>	
<b>Service ID [hex]</b>	0x10	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for the same cryptoKeyId	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key whose key element shall be the source element.
	targetCryptoKeyId	Holds the identifier of the key whose key element shall be the destination element.

<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_Return-Type	<p>E_OK: Request successful  E_NOT_OK: Request failed  CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy  CRYPTO_E_KEY_NOT_AVAILABLE: Request failed, the requested key element is not available  CRYPTO_E_KEY_READ_FAIL: Request failed, not allowed to extract key element  CRYPTO_E_KEY_WRITE_FAIL: Request failed, not allowed to write key element  CRYPTO_E_KEY_SIZE_MISMATCH: Request failed, key element sizes are not compatible  CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element</p>
<b>Description</b>	Copies a key with all its elements to another key in the same crypto driver. Note: If the actual key element is directly mapped to flash memory, there could be a bigger delay when calling this function (synchronous operation)	
<b>Available via</b>	Crypto.h	

l()

**[SWS\_Crypto\_00156]** [ If the Crypto Driver is not yet initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyCopy` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00157]** [ If `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyCopy` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00158]** [ If `targetCryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyCopy` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00159]** If no errors are detected by the Crypto Driver, the function shall copy all key elements in the key referenced by `cryptoKeyId` to the key the key referenced by `targetCryptoKeyId`.

l()

#### 8.3.4.3.4 `Crypto_KeyElementIdsGet`

**[SWS\_Crypto\_00160]**

<b>Service</b>	<code>Crypto_KeyElementIdsGet</code>
----------------	--------------------------------------

<b>Name</b>		
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyElementIdsGet (     uint32 cryptoKeyId,     uint32* keyElementIdsPtr,     uint32* keyElementIdsLengthPtr )</pre>	
<b>Service ID [hex]</b>	0x11	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for the same cryptoKeyId	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key whose available element ids shall be exported.
	keyElementIdsLengthPtr	Holds a pointer to the memory location in which the number of key elements in the given key is stored. On calling this function, this parameter shall contain the size of the buffer provided by keyElementIdsPtr. When the request has finished, the actual number of key elements shall be stored.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	keyElementIdsPtr	Contains the pointer to the array where the ids of the key elements shall be stored.
<b>Return value</b>	Std_ReturnType	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy
<b>Description</b>	Used to retrieve information which key elements are available in a given key.	
<b>Available via</b>	Crypto.h	

l()

**[SWS\_Crypto\_00161]** [ If the Crypto Driver is not yet initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementIdsGet` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00162]** [ If `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyElementIdsGet` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

If no errors are detected by the Crypto Driver, the function stores all ids of the key elements available in the key identified by `cryptoKeyId` to an array provided by `keyElementIdsPtr`. It also stores the number of elements to the value, which is pointed by `keyElementIdsLengthPtr`.

Note: This function is needed by the CRYIF when a whole key should be copied from one Crypto Driver to another Crypto Driver by the CRYIF.

### 8.3.4.4 Key Generation Interface

#### 8.3.4.4.1 Crypto\_RandomSeed

[SWS\_Crypto\_91013]

<b>Service Name</b>	Crypto_RandomSeed	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_RandomSeed (     uint32 cryptoKeyId,     const uint8* seedPtr,     uint32 seedLength )</pre>	
<b>Service ID [hex]</b>	0x0d	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant, but not for the same cryptoKeyId	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key for which a new seed shall be generated.
	seedPtr	Holds a pointer to the memory location which contains the data to feed the seed.
	seedLength	Contains the length of the seed in bytes.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_ReturnType	E_OK: Request successful E_NOT_OK: Request failed
<b>Description</b>	This function generates the internal seed state using the provided entropy source. Furthermore, this function can be used to update the seed state with new entropy	
<b>Available via</b>	Crypto.h	

l()

[SWS\_Crypto\_00128] [ If the module is not yet initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_RandomSeed` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

[SWS\_Crypto\_00129] [ If the parameter `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_RandomSeed` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00130]** [ If the parameter `seedPtr` is a null pointer and if development error detection for the Crypto Driver is enabled, the function `Crypto_RandomSeed` shall report `CRYPTO_E_PARAM_POINTER` to the DET and return `E_NOT_OK`.

]()

**[SWS\_Crypto\_00131]** [ If `seedLength` is zero and if development error detection for the Crypto Driver is enabled, the function `Crypto_RandomSeed` shall report `CRYPTO_E_PARAM_VALUE` to the DET and return `E_NOT_OK`.

]()

If no errors are detected by Crypto Driver, the service `Crypto_RandomSeed()` feeds the given key with a seed state derived from the entropy source. The internal state of the random generator is stored in the key element `CRYPTO_KE_RANDOM_SEED`.

#### 8.3.4.4.2 Crypto\_KeyGenerate

**[SWS\_Crypto\_91007]**[

<b>Service Name</b>	Crypto_KeyGenerate	
<b>Syntax</b>	Std_ReturnType Crypto_KeyGenerate ( uint32 cryptoKeyId )	
<b>Service ID [hex]</b>	0x07	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for the same cryptoKeyId	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key which is to be updated with the generated value.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_Return-Type	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element
<b>Description</b>	Generates new key material store it in the key identified by cryptoKeyId.	
<b>Available via</b>	Crypto.h	

]()

**[SWS\_Crypto\_00094]** [ If the module is not yet initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyGenerate` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

]()

**[SWS\_Crypto\_00095]** [ If the parameter `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyGenerate` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

]()

**[SWS\_Crypto\_00165]** [ If no errors are detected by Crypto Driver, the service `Crypto_KeyGenerate()` generates the corresponding key.

]()

### 8.3.4.5 Key Derivation Interface

#### 8.3.4.5.1 Crypto\_KeyDerive

**[SWS\_Crypto\_91008]**[

<b>Service Name</b>	Crypto_KeyDerive	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyDerive (     uint32 cryptoKeyId,     uint32 targetCryptoKeyId )</pre>	
<b>Service ID [hex]</b>	0x08	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for the same cryptoKeyId	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key which is used for key derivation.
	targetCryptoKeyId	Holds the identifier of the key which is used to store the derived key.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_ReturnType	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element
<b>Description</b>	Derives a new key by using the key elements in the given key identified by the crypto KeyId. The given key contains the key elements for the password, salt. The derived	

	key is stored in the key element with the id 1 of the key identified by targetCryptoKeyId. The number of iterations is given in the key element CRYPTO_KEY_DERIVATION_ITERATIONS.
<b>Available via</b>	Crypto.h

}]()

**[SWS\_Crypto\_00097]** [ If the module is not yet initialized and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyDerive` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

}]()

**[SWS\_Crypto\_00098]** [ If the parameter `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyDerive` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

}]()

**[SWS\_Crypto\_00180]** [ If the parameter `targetCryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyDerive` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.] ()

**[SWS\_Crypto\_00166]** [ If no errors are detected by Crypto Driver, the service `Crypto_KeyDerive()` derives a key element with the aid of a salt and a password. ]()

The key derivation service needs a salt and password to derivate a new key. The salt and the password therefore are stored as key elements in the key referred by `cryptoKeyId`.

### 8.3.4.6 Key Exchange Interface

#### 8.3.4.6.1 Crypto\_KeyExchangeCalcPubVal

**[SWS\_Crypto\_91009]**

<b>Service Name</b>	Crypto_KeyExchangeCalcPubVal	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyExchangeCalcPubVal (     uint32 cryptoKeyId,     uint8* publicValuePtr,     uint32* publicValueLengthPtr )</pre>	
<b>Service ID [hex]</b>	0x09	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for the same <code>cryptoKeyId</code>	
<b>Parameters</b>	<code>cryptoKey</code>	Holds the identifier of the key which shall be used for the key exchange

<b>(in)</b>	Id	protocol.
<b>Parameters (inout)</b>	public Value LengthPtr	Holds a pointer to the memory location in which the public value length information is stored. On calling this function, this parameter shall contain the size of the buffer provided by publicValuePtr. When the request has finished, the actual length of the returned value shall be stored.
<b>Parameters (out)</b>	public ValuePtr	Contains the pointer to the data where the public value shall be stored.
<b>Return value</b>	Std_- Return-Type	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element
<b>Description</b>	Calculates the public value for the key exchange and stores the public key in the memory location pointed by the public value pointer.	
<b>Available via</b>	Crypto.h	

l()

**[SWS\_Crypto\_00103]** [ If the module is not yet initialized and if development error detection for the Crypto Driver is enabled: The function

`Crypto_KeyExchangeCalcPubVal` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00104]** [ If the parameter `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyExchangeCalcPubVal` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00105]** [ If the parameter `publicValuePtr` is a null pointer and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyExchangeCalcPubVal` shall report `CRYPTO_E_PARAM_POINTER` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00106]** [ If the parameter `pubValueLengthPtr` is a null pointer and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyExchangeCalcPubVal` shall report `CRYPTO_E_PARAM_POINTER` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00107]** [ If the value, which is pointed by `pubValueLengthPtr` is zero and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyExchangeCalcPubVal` shall report `CRYPTO_E_PARAM_VALUE` to the DET and return `E_NOT_OK`.



l()

**[SWS\_Crypto\_00167]** [ If no errors are detected by Crypto Driver, the service `Crypto_KeyExchangeCalcPubVal()` calculates the public value of the current job for the key exchange.

l()

**[SWS\_Crypto\_00109]** [ The pointer `publicValuePtr` holds the memory location, where the data of the public value shall be stored. On calling this function, `publicValueLengthPtr` shall contain the size of the buffer provided by `publicValuePtr`. When the request has finished, the actual length of the returned value shall be stored.

l()

### 8.3.4.6.2 Crypto\_KeyExchangeCalcSecret

**[SWS\_Crypto\_91010]**[

<b>Service Name</b>	Crypto_KeyExchangeCalcSecret	
<b>Syntax</b>	<pre>Std_ReturnType Crypto_KeyExchangeCalcSecret (     uint32 cryptoKeyId,     const uint8* partnerPublicValuePtr,     uint32 partnerPublicValueLength )</pre>	
<b>Service ID [hex]</b>	0x0a	
<b>Sync/Async</b>	Synchronous	
<b>Reentrancy</b>	Reentrant but not for the same cryptoKeyId	
<b>Parameters (in)</b>	cryptoKeyId	Holds the identifier of the key which shall be used for the key exchange protocol.
	partnerPublicValuePtr	Holds the pointer to the memory location which contains the partner's public value.
	partnerPublicValueLength	Contains the length of the partner's public value in bytes.
<b>Parameters (inout)</b>	None	
<b>Parameters (out)</b>	None	
<b>Return value</b>	Std_ReturnType	E_OK: Request successful E_NOT_OK: Request failed CRYPTO_E_BUSY: Request failed, Crypto Driver Object is busy CRYPTO_E_SMALL_BUFFER: The provided buffer is too small to store the result CRYPTO_E_KEY_EMPTY: Request failed because of uninitialized source key element

<b>Description</b>	Calculates the shared secret key for the key exchange with the key material of the key identified by the cryptoKeyId and the partner public key. The shared secret key is stored as a key element in the same key.
<b>Available via</b>	Crypto.h

l()

**[SWS\_Crypto\_00111]** [ If the module is not yet initialized and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyExchangeCalcSecret` shall report `CRYPTO_E_UNINIT` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00112]** [ If the parameter `cryptoKeyId` is out of range and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyExchangeCalcSecret` shall report `CRYPTO_E_PARAM_HANDLE` to the DET and return `E_NOT_OK`

l()

**[SWS\_Crypto\_00113]** [ If the parameter `partnerPublicValuePtr` is a null pointer and if development error detection for the Crypto Driver is enabled, the function `Crypto_KeyExchangeCalcSecret` shall report

`CRYPTO_E_PARAM_POINTER` to the DET and return `E_NOT_OK`.

l()

**[SWS\_Crypto\_00115]** [ If `partnerPublicValueLength` is zero and if development error detection for the Crypto Driver is enabled, the function

`Crypto_KeyExchangeCalcSecret` shall report `CRYPTO_E_PARAM_VALUE` to the DET and return `E_NOT_OK`.

l()

If no errors are detected by Crypto, the service

`Crypto_KeyExchangeCalcSecret()` calculated the shared secret key for the key exchange and store it as key element in `cryptoKeyId`.

## 8.4 Scheduled functions

### 8.4.1.1 Crypto\_MainFunction

The `Crypto_MainFunction()` is necessary for asynchronous job processing. For synchronous job processing providing the main function is optional.

**[SWS\_Crypto\_91012]**[

<b>Service Name</b>	Crypto_MainFunction
<b>Syntax</b>	void Crypto_MainFunction ( void )
<b>Service ID [hex]</b>	0x0c
<b>Description</b>	If asynchronous job processing is configured and there are job queues, the function is called cyclically to process queued jobs.
<b>Available via</b>	SchM_Crypto.h

]()

## 8.5 Expected Interfaces

In this section, all interfaces required from other modules are listed.

### 8.5.1 Interfaces to Standard Software Modules

**[SWS\_Crypto\_00126]** [ The Crypto Driver shall use an AUTOSAR DET module for development error notification.

]()

### 8.5.2 Mandatory Interfaces

[[

<b>API Function</b>	<b>Header File</b>	<b>Description</b>
There are no mandatory interfaces.		

]()

### 8.5.3 Optional Interfaces

**[SWS\_Crypto\_91017]**[

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

]()

## 9 Sequence diagrams

n/a

## 10 Configuration specification

Chapter 10.1 specifies the structure (containers) and the parameters of the module Crypto.

Chapter 10.2 specifies additionally published information of the module Crypto.

### 10.1 Containers and configuration parameters

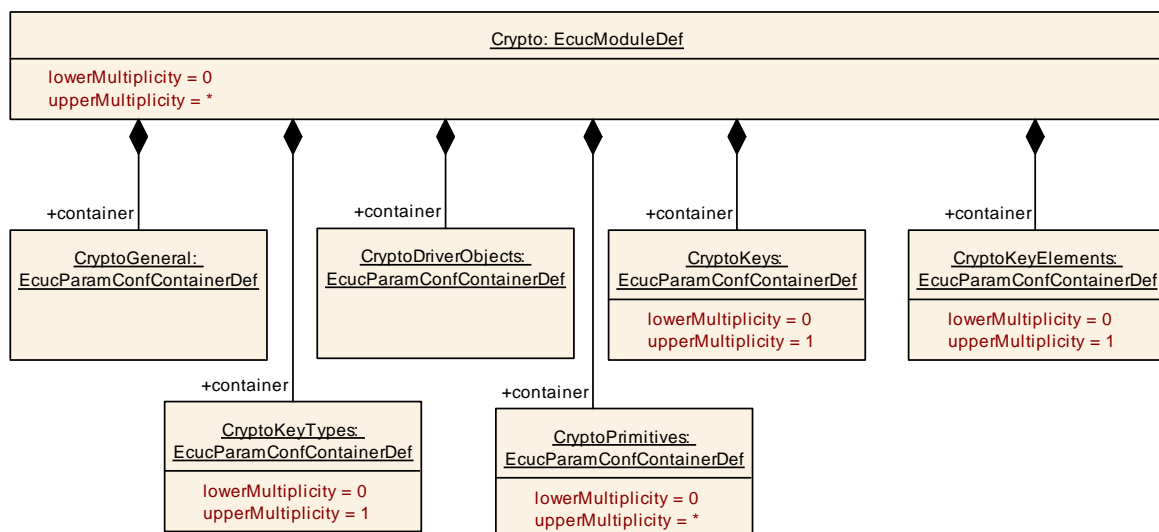
The following chapters summarize all configuration parameters. The detailed meanings of the parameters describe Chapters 7 and Chapter 8.

Note: The Ids in the configuration containers shall be consecutive, gapless and shall start from zero.

#### 10.1.1 Crypto

<b>SWS Item</b>	<b>ECUC_Crypto_00001 :</b>
<b>Module Name</b>	<i>Crypto</i>
<b>Module Description</b>	Configuration of the Crypto (CryptoDriver) module
<b>Post-Build Variant Support</b>	false
<b>Supported Config Variants</b>	VARIANT-PRE-COMPILE

<b>Included Containers</b>		
<b>Container Name</b>	<b>Multiplicity</b>	<b>Scope / Dependency</b>
CryptoDriverObjects	1	Container for CRYPTO Objects
CryptoGeneral	1	Container for common configuration options
CryptoKeyElements	0..1	Container for Crypto key elements
CryptoKeyTypes	0..1	Container for CRYPTO key types
CryptoKeys	0..1	Container for CRYPTO keys
CryptoPrimitives	0..*	Container for CRYPTO primitives



## 10.1.2 CryptoGeneral

<b>SWS Item</b>	<b>ECUC_Crypto_00002 :</b>		
<b>Container Name</b>	CryptoGeneral		
<b>Parent Container</b>	Crypto		
<b>Description</b>	Container for common configuration options		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Configuration Parameters</b>			

<b>SWS Item</b>	<b>ECUC_Crypto_00006 :</b>		
<b>Name</b>	CryptoDevErrorDetect		
<b>Parent Container</b>	CryptoGeneral		
<b>Description</b>	Switches the development error detection and notification on or off. true: detection and notification is enabled. false: detection and notification is disabled		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucBooleanParamDef		
<b>Default value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00040 :</b>		
<b>Name</b>	CryptoInstancelD		
<b>Parent Container</b>	CryptoGeneral		
<b>Description</b>	Instance ID of the crypto driver. This ID is used to discern several crypto drivers in case more than one driver is used in the same ECU.		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucIntegerParamDef		
<b>Range</b>	0 .. 255		
<b>Default value</b>	--		
<b>Post-Build Variant Value</b>	false		
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00038 :</b>		
<b>Name</b>	CryptoMainFunctionPeriod		
<b>Parent Container</b>	CryptoGeneral		
<b>Description</b>	Specifies the period of main function Crypto_MainFunction in seconds.		
<b>Multiplicity</b>	0..1		
<b>Type</b>	EcucFloatParamDef		
<b>Range</b>	]0 .. INF[		
<b>Default value</b>	--		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	

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

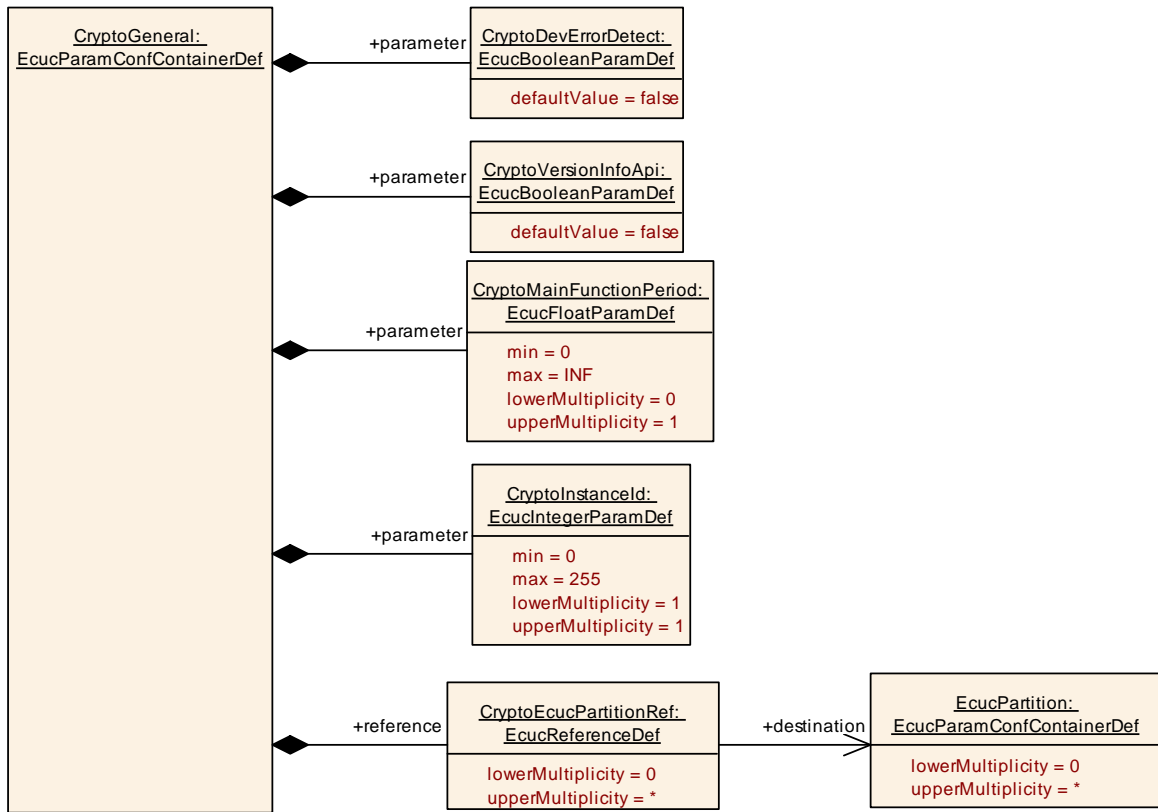
<b>SWS Item</b>	<b>ECUC_Crypto_00007 :</b>		
<b>Name</b>	CryptoVersionInfoApi		
<b>Parent Container</b>	CryptoGeneral		
<b>Description</b>	Pre-processor switch to enable and disable availability of the API Crypto_GetVersionInfo(). True: API Crypto_GetVersionInfo() is available False: API Cryptosm_GetVersionInfo() is not available.		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucBooleanParamDef		
<b>Default value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00042 :</b>		
<b>Name</b>	CryptoEcucPartitionRef		
<b>Parent Container</b>	CryptoGeneral		
<b>Description</b>	Maps the Crypto driver to zero or multiple ECUC partitions to make the modules API available in this partition. The module will operate as an independent instance in each of the partitions.		
<b>Multiplicity</b>	0..*		
<b>Type</b>	Reference to [ EcucPartition ]		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Post-Build Variant Value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: ECU		

**No Included Containers**

**[SWS\_Crypto\_00212]** | The Crypto Driver module shall reject configurations with partition mappings which are not supported by the implementation.  
 |()

**[SWS\_Crypto\_CONSTR\_00001]** | The Crypto Driver module will operate as an independent instance in each of the partitions, means the called API will only target the partition it is called in.  
 |()

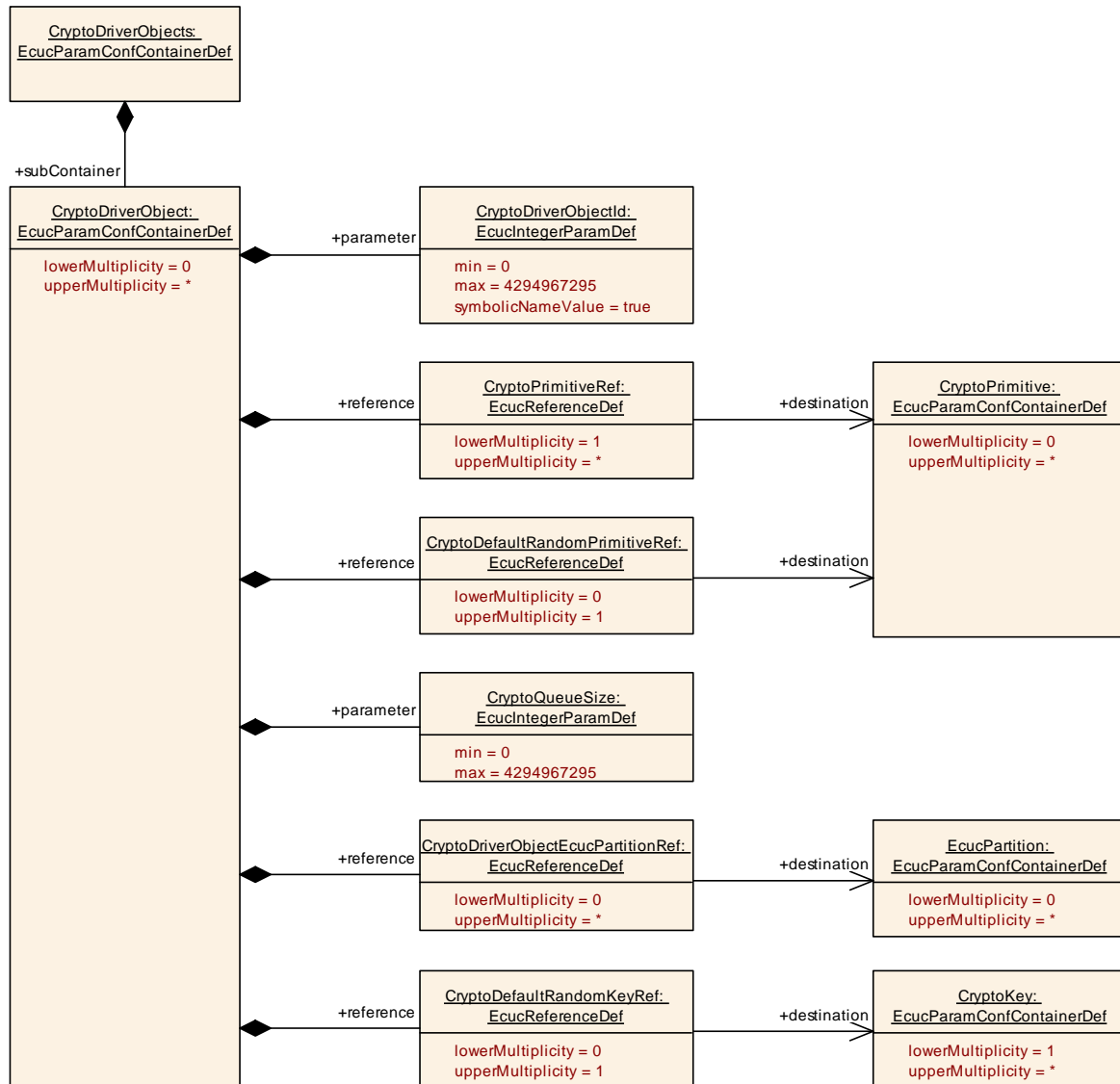


### 10.1.3 CryptoDriverObjects

SWS Item	ECUC_Crypto_0003 :		
Container Name	CryptoDriverObjects		
Parent Container	Crypto		
Description	Container for CRYPTO Objects		
Post-Build Variant	false		
Multiplicity Configuration	Pre-compile time	X	All Variants
Class	Link time	--	
	Post-build time	--	
Configuration Parameters			

Included Containers		
Container Name	Multiplicity	Scope / Dependency
CryptoDriverObject	0..*	Configuration of a CryptoDriverObject





### 10.1.4 CryptoDriverObject

<b>SWS Item</b>	<b>ECUC_Crypto_00008 :</b>
<b>Container Name</b>	CryptoDriverObject
<b>Parent Container</b>	CryptoDriverObjects
<b>Description</b>	Configuration of a CryptoDriverObject
<b>Configuration Parameters</b>	

<b>SWS Item</b>	<b>ECUC_Crypto_00009 :</b>
<b>Name</b>	CryptoDriverObjectId
<b>Parent Container</b>	CryptoDriverObject
<b>Description</b>	Identifier of the Crypto Driver Object. The Crypto Driver Object offers different crypto primitives.
<b>Multiplicity</b>	1
<b>Type</b>	EcucIntegerParamDef (Symbolic Name generated for this parameter)
<b>Range</b>	0 .. 4294967295

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

<b>SWS Item</b>	<b>ECUC_Crypto_00019 :</b>		
<b>Name</b>	CryptoQueueSize		
<b>Parent Container</b>	CryptoDriverObject		
<b>Description</b>	Size of the queue in the Crypto Driver. Defines the maximum number of jobs in the Crypto Driver Object queue. If it is set to 0, queueing is disabled in the Crypto Driver Object.		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucIntegerParamDef		
<b>Range</b>	0 .. 4294967295		
<b>Default value</b>	--		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00045 :</b>		
<b>Name</b>	CryptoDefaultRandomKeyRef		
<b>Parent Container</b>	CryptoDriverObject		
<b>Description</b>	This is a reference to the CryptoKey that is used by the CryptoDefaultRandomPrimitiveRef. The key contains key elements that are necessary to seed the random number generator. This element shall only be set if the primitive referenced by CryptoDefaultRandomPrimitiveRef requires a seed value.		
<b>Multiplicity</b>	0..1		
<b>Type</b>	Reference to [ CryptoKey ]		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00044 :</b>		
<b>Name</b>	CryptoDefaultRandomPrimitiveRef		
<b>Parent Container</b>	CryptoDriverObject		
<b>Description</b>	This is a reference to a primitive that configures a default random number generator. If a crypto driver object needs to perform a crypto primitive that requires a random number generator, but the configuration of this primitive does not provide parameter for a random number generator, then this default random number generator shall be used (i.e. the elements of		

	algorithm family, secondary algorithm family and algorithm mode do not provide this information). Example: The crypto driver shall generate a signature based on elliptic curve but the primitive for signature generation lacks information about a random number generator.		
<b>Multiplicity</b>	0..1		
<b>Type</b>	Reference to [ CryptoPrimitive ]		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00043 :</b>		
<b>Name</b>	CryptoDriverObjectEcucPartitionRef		
<b>Parent Container</b>	CryptoDriverObject		
<b>Description</b>	Maps a crypto driver object to zero or multiple ECUC partitions. The ECUC partition referenced is a subset of the ECUC partitions where the Crypto driver is mapped to. Note: CryptoDriverObjects such as a HSM shall be mapped to one partition only.		
<b>Multiplicity</b>	0..*		
<b>Type</b>	Reference to [ EcucPartition ]		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Post-Build Variant Value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: ECU		

<b>SWS Item</b>	<b>ECUC_Crypto_00018 :</b>		
<b>Name</b>	CryptoPrimitiveRef		
<b>Parent Container</b>	CryptoDriverObject		
<b>Description</b>	Refers to primitive in the CRYPTO. The CryptoPrimitive is a pre-configured container of the crypto service that shall be used.		
<b>Multiplicity</b>	1..*		
<b>Type</b>	Reference to [ CryptoPrimitive ]		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Post-Build Variant Value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

**No Included Containers**

**[SWS\_Crypto\_CONSTR\_00002]** | The ECUC partitions referenced by CryptoDriverObjectEcucPartitionRef shall be a subset of the ECUC partitions referenced by CryptoEcucPartitionRef.

l()

**[SWS\_Crypto\_CONSTR\_00003]** | If the CryptoDriverObjectEcucPartitionRef shall be configured for an HSM it shall be mapped to 0 or 1 ECUC partitions only.

l()

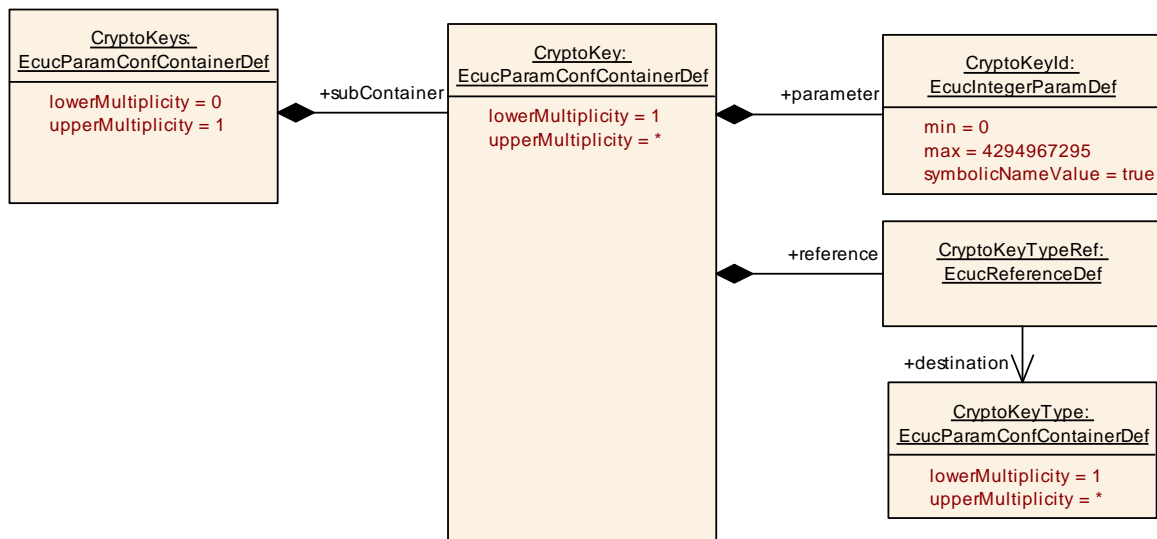
**[SWS\_Crypto\_CONSTR\_00004]** | If CryptoEcucPartitionRef references one or more ECUC partitions, CryptoDriverObjectEcucPartitionRef shall have a multiplicity of greater than zero and reference one or several of these ECUC partitions as well.

l()

### 10.1.5 CryptoKeys

<b>SWS Item</b>	<b>ECUC_Crypto_00004 :</b>
<b>Container Name</b>	CryptoKeys
<b>Parent Container</b>	Crypto
<b>Description</b>	Container for CRYPTO keys
<b>Configuration Parameters</b>	

<b>Included Containers</b>		
<b>Container Name</b>	<b>Multiplicity</b>	<b>Scope / Dependency</b>
CryptoKey	1..*	Configuration of a CryptoKey



### 10.1.6 CryptoKey

<b>SWS Item</b>	<b>ECUC_Crypto_00011 :</b>		
<b>Container Name</b>	CryptoKey		
<b>Parent Container</b>	CryptoKeys		
<b>Description</b>	Configuration of a CryptoKey		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Configuration Parameters</b>			

<b>SWS Item</b>	<b>ECUC_Crypto_00012 :</b>		
<b>Name</b>	CryptoKeyId		
<b>Parent Container</b>	CryptoKey		
<b>Description</b>	Identifier of the CRYPTO Key		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
<b>Range</b>	0 .. 4294967295		
<b>Default value</b>	--		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Post-Build Variant Value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

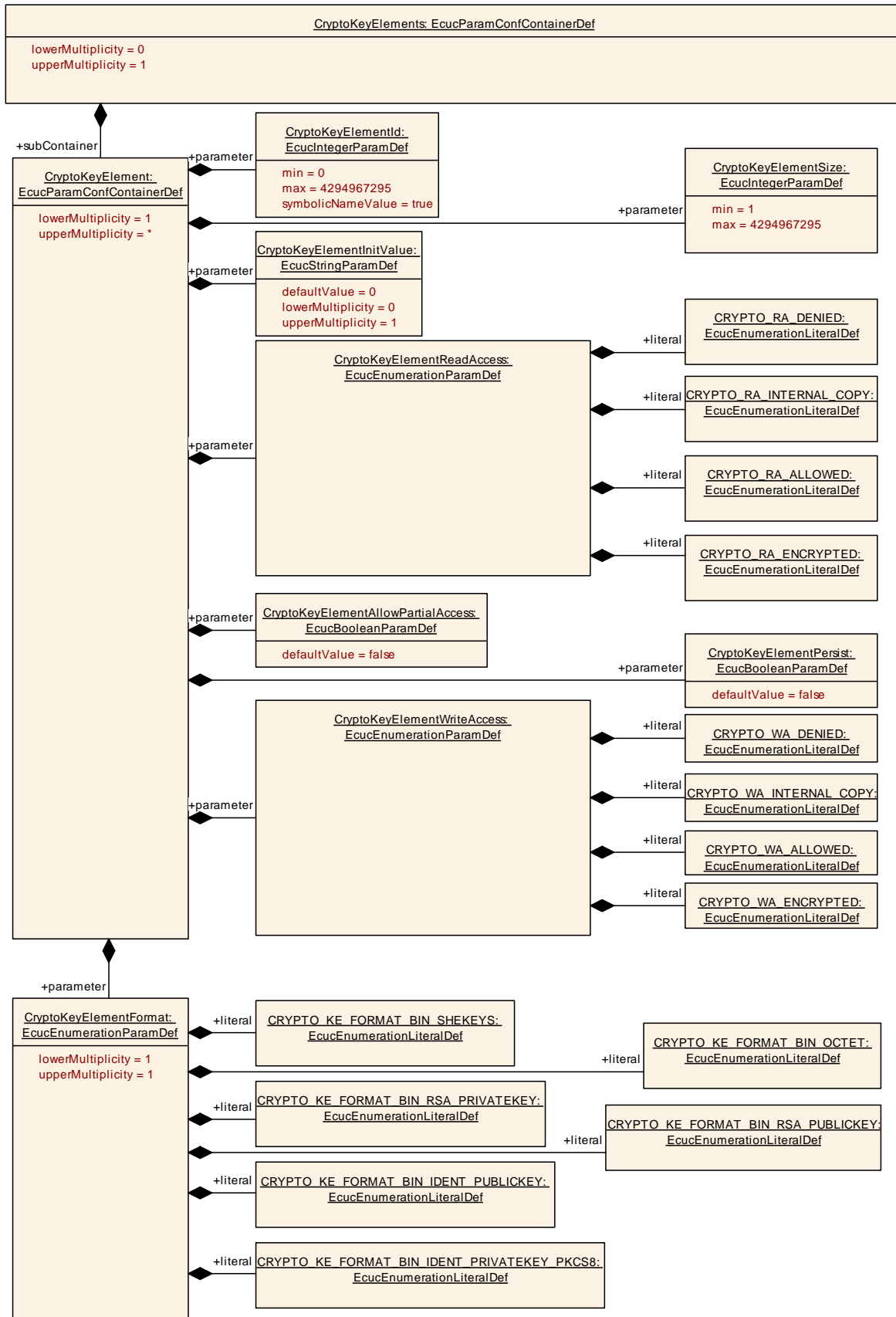
<b>SWS Item</b>	<b>ECUC_Crypto_00020 :</b>		
<b>Name</b>	CryptoKeyTypeRef		
<b>Parent Container</b>	CryptoKey		
<b>Description</b>	Refers to a pointer in the CRYPTO to a CryptoKeyType. The CryptoKeyType provides the information which key elements are contained in a CryptoKey.		
<b>Multiplicity</b>	1		
<b>Type</b>	Reference to [ CryptoKeyType ]		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Post-Build Variant Value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

**No Included Containers**

### 10.1.7 CryptoKeyElements

<b>SWS Item</b>	<b>ECUC_Crypto_00005 :</b>
<b>Container Name</b>	CryptoKeyElements
<b>Parent Container</b>	Crypto
<b>Description</b>	Container for Crypto key elements
<b>Configuration Parameters</b>	

<b>Included Containers</b>		
<b>Container Name</b>	<b>Multiplicity</b>	<b>Scope / Dependency</b>
CryptoKeyElement	1..*	Configuration of a CryptoKeyElement



### 10.1.8 CryptoKeyElement

<b>SWS Item</b>	<b>ECUC_Crypto_00014 :</b>
<b>Container Name</b>	CryptoKeyElement
<b>Parent Container</b>	CryptoKeyElements
<b>Description</b>	Configuration of a CryptoKeyElement
<b>Configuration Parameters</b>	

<b>SWS Item</b>	<b>ECUC_Crypto_00025 :</b>		
<b>Name</b>	CryptoKeyElementAllowPartialAccess		
<b>Parent Container</b>	CryptoKeyElement		
<b>Description</b>	Enable or disable writing and reading the key element with data smaller than the size of the element. True: enable partial access of the key element False: disable partial access of the key element		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucBooleanParamDef		
<b>Default value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00041 :</b>		
<b>Name</b>	CryptoKeyElementFormat		
<b>Parent Container</b>	CryptoKeyElement		
<b>Description</b>	Defines the format for the key element. This is the format used to provide or extract the key data from the driver.		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucEnumerationParamDef		
<b>Range</b>	CRYPTO_KEY_FORMAT_BIN_IDENT_PRIVATEKEY_PKCS8	0x03	
	CRYPTO_KEY_FORMAT_BIN_IDENT_PUBLICKEY	0x04	
	CRYPTO_KEY_FORMAT_BIN_OCTET	0x01	
	CRYPTO_KEY_FORMAT_BIN_RSA_PRIVATEKEY	0x05	
	CRYPTO_KEY_FORMAT_BIN_RSA_PUBLICKEY	0x06	
	CRYPTO_KEY_FORMAT_BIN_SHEKEYS	0x02	
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>			

<b>SWS Item</b>	<b>ECUC_Crypto_00021 :</b>		
<b>Name</b>	CryptoKeyElementId		
<b>Parent Container</b>	CryptoKeyElement		
<b>Description</b>	Identifier of the CRYPTO key element		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucIntegerParamDef (Symbolic Name generated for this parameter)		
<b>Range</b>	0 .. 4294967295		



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

<b>SWS Item</b>	<b>ECUC_Crypto_00023 :</b>		
<b>Name</b>	CryptoKeyElementInitValue		
<b>Parent Container</b>	CryptoKeyElement		
<b>Description</b>	Value which will be used to fill the key element during startup (i) for all non-persistent key elements, and (ii) for those persistent key elements that have never been written.		
<b>Multiplicity</b>	0..1		
<b>Type</b>	EcucStringParamDef		
<b>Default value</b>	0		
<b>maxLength</b>	--		
<b>minLength</b>	--		
<b>regularExpression</b>	--		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00026 :</b>		
<b>Name</b>	CryptoKeyElementPersist		
<b>Parent Container</b>	CryptoKeyElement		
<b>Description</b>	Enable or disable persisting of the key element in non-volatile storage. True: enable persisting of the key element. False: disable persisting of the key element.		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucBooleanParamDef		
<b>Default value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00024 :</b>		
<b>Name</b>	CryptoKeyElementReadAccess		
<b>Parent Container</b>	CryptoKeyElement		
<b>Description</b>	Define the reading access rights of the key element through external API. CRYPTO_RA_DENIED = key element cannot be read from outside the Crypto Driver CRYPTO_RA_INTERNAL_COPY = key element can be copied to another key		

	element in the same crypto driver. CRYPTO_RA_ALLOWED = key element can be read as plaintext CRYPTO_RA_ENCRYPTED = key element can be read encrypted. E.g. SHE Ram-Key export.		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucEnumerationParamDef		
<b>Range</b>	CRYPTO_RA_ALLOWED	0x00	
	CRYPTO_RA_DENIED	0x03	
	CRYPTO_RA_ENCRYPTED	0x01	
	CRYPTO_RA_INTERNAL_COPY	0x02	
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local dependency: The values for the enumeration types are chosen in a way that its value can be used to deduce a hierarchical access level.		

<b>SWS Item</b>	<b>ECUC_Crypto_00022 :</b>		
<b>Name</b>	CryptoKeyElementSize		
<b>Parent Container</b>	CryptoKeyElement		
<b>Description</b>	Maximum Size size of a CRYPTO key element in bytes		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucIntegerParamDef		
<b>Range</b>	1 .. 4294967295		
<b>Default value</b>	--		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Post-Build Variant Value</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

<b>SWS Item</b>	<b>ECUC_Crypto_00027 :</b>		
<b>Name</b>	CryptoKeyElementWriteAccess		
<b>Parent Container</b>	CryptoKeyElement		
<b>Description</b>	Define the writing access rights of the key element through external API. CRYPTO_WA_DENIED = key element can not be written from outside the Crypto Driver CRYPTO_WA_INTERNAL_COPY = key element can be filled with another key element in the same crypto driver. CRYPTO_WA_ALLOWED = key element can be rwritten as plaintext CRYPTO_WA_ENCRYPTED = key element can be written encrypted. E.g. SHE load key.		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucEnumerationParamDef		
<b>Range</b>	CRYPTO_WA_ALLOWED	0x00	
	CRYPTO_WA_DENIED	0x03	
	CRYPTO_WA_ENCRYPTED	0x01	
	CRYPTO_WA_INTERNAL_COPY	0x02	

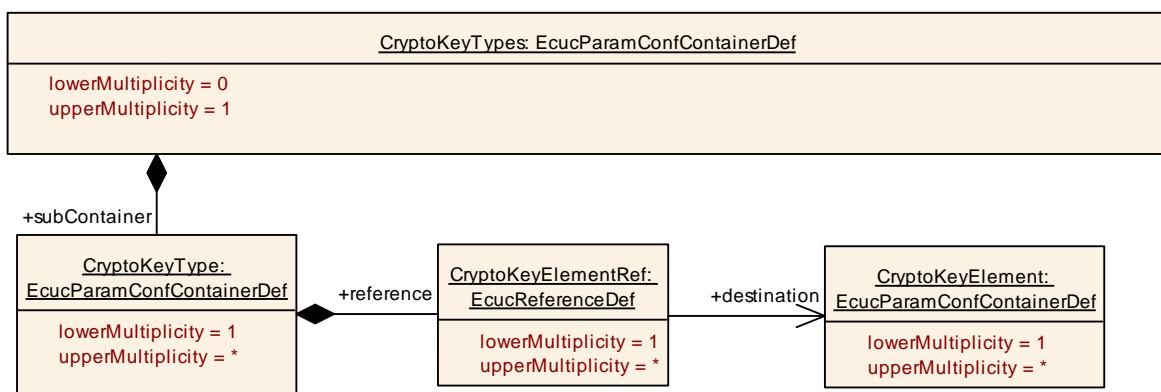
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local dependency: The values for the enumeration types are chosen in a way that its value can be used to deduce a hierarchical access level.		

**No Included Containers**

### 10.1.9 CryptoKeyTypes

<b>SWS Item</b>	<b>ECUC_Crypto_00017 :</b>		
<b>Container Name</b>	CryptoKeyTypes		
<b>Parent Container</b>	Crypto		
<b>Description</b>	Container for CRYPTO key types		
<b>Post-Build Variant Multiplicity</b>	false		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Configuration Parameters</b>			

<b>Included Containers</b>		
<b>Container Name</b>	<b>Multiplicity</b>	<b>Scope / Dependency</b>
CryptoKeyType	1..*	Configuration of a CryptoKeyType



### 10.1.10 CryptoKeyType

<b>SWS Item</b>	<b>ECUC_Crypto_00030 :</b>
<b>Container Name</b>	CryptoKeyType
<b>Parent Container</b>	CryptoKeyTypes
<b>Description</b>	Configuration of a CryptoKeyType

**Configuration Parameters**

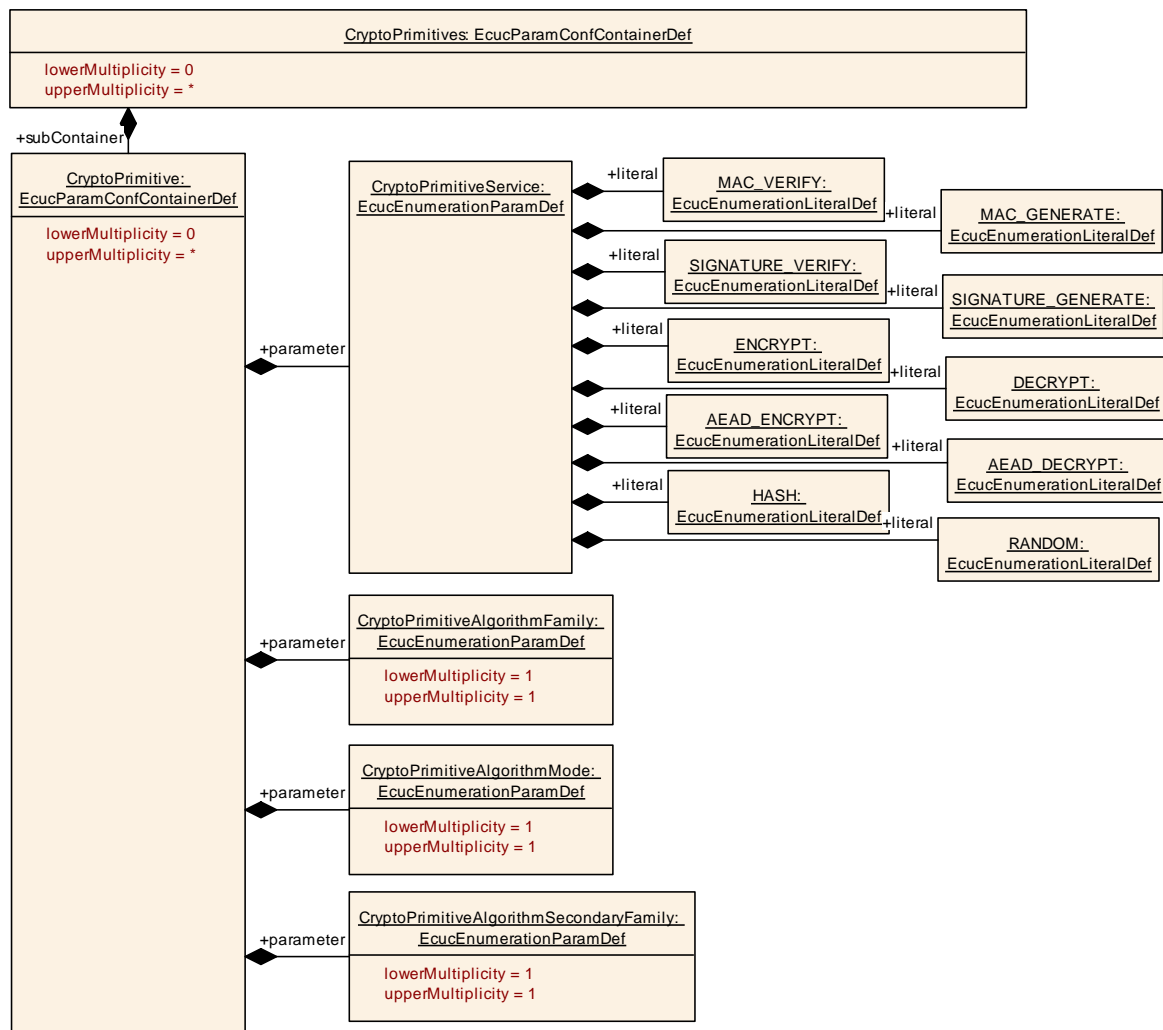
<b>SWS Item</b>	<b>ECUC_Crypto_00031 :</b>		
<b>Name</b>	CryptoKeyElementRef		
<b>Parent Container</b>	CryptoKeyType		
<b>Description</b>	Refers to a pointer in the CRYPTO Crypto Key Element, which holds the data of the crypto key element.		
<b>Multiplicity</b>	1..*		
<b>Type</b>	Reference to [ CryptoKeyElement ]		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Scope / Dependency</b>	scope: local		

**No Included Containers**

### 10.1.11 CryptoPrimitives

<b>SWS Item</b>	<b>ECUC_Crypto_00032 :</b>		
<b>Container Name</b>	CryptoPrimitives		
<b>Parent Container</b>	Crypto		
<b>Description</b>	Container for CRYPTO primitives		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Configuration Parameters</b>			

<b>Included Containers</b>		
<b>Container Name</b>	<b>Multiplicity</b>	<b>Scope / Dependency</b>
CryptoPrimitive	0..*	Configuration of a CryptoPrimitive



### 10.1.12 CryptoPrimitive

<b>SWS Item</b>	<b>ECUC_Crypto_00033 :</b>		
<b>Container Name</b>	CryptoPrimitive		
<b>Parent Container</b>	CryptoPrimitives		
<b>Description</b>	Configuration of a CryptoPrimitive		
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X	All Variants
	<b>Link time</b>	--	
	<b>Post-build time</b>	--	
<b>Configuration Parameters</b>			

<b>SWS Item</b>	<b>ECUC_Crypto_00035 :</b>		
<b>Name</b>	CryptoPrimitiveAlgorithmFamily		
<b>Parent Container</b>	CryptoPrimitive		
<b>Description</b>	Determines the algorithm family used for the crypto service		
<b>Multiplicity</b>	1		
<b>Type</b>	EcucEnumerationParamDef		
<b>Range</b>	CRYPTO_ALGOFAM_3DES		0x13
	CRYPTO_ALGOFAM_AES		0x14
	CRYPTO_ALGOFAM_BLAKE_1_256		0x0F

	CRYPTO_ALGOFAM_BLAKE_1_512	0x10
	CRYPTO_ALGOFAM_BLAKE_2s_256	0x11
	CRYPTO_ALGOFAM_BLAKE_2s_512	0x12
	CRYPTO_ALGOFAM_BRAINPOOL	0x18
	CRYPTO_ALGOFAM_CHACHA	0x15
	CRYPTO_ALGOFAM_CUSTOM	0xFF
	CRYPTO_ALGOFAM_DH	0x26
	CRYPTO_ALGOFAM_DRBG	0x20
	CRYPTO_ALGOFAM_ECCANSI	0x1e
	CRYPTO_ALGOFAM_ECCNIST	0x19
	CRYPTO_ALGOFAM_ECCSEC	0x1f
	CRYPTO_ALGOFAM_ED25519	0x17
	CRYPTO_ALGOFAM_FIPS186	0x21
	CRYPTO_ALGOFAM_KDFX963	0x25
	CRYPTO_ALGOFAM_NOT_SET	0x00
	CRYPTO_ALGOFAM_PADDING_ONEWITHZEROS	0x23
	CRYPTO_ALGOFAM_PADDING_PKCS7	0x22
	CRYPTO_ALGOFAM_PBKDF2	0x24
	CRYPTO_ALGOFAM_RIPEMD160	0x0E
	CRYPTO_ALGOFAM_RNG	0x1B
	CRYPTO_ALGOFAM_RSA	0x16
	CRYPTO_ALGOFAM_SHA1	0x01
	CRYPTO_ALGOFAM_SHA2_224	0x02
	CRYPTO_ALGOFAM_SHA2_256	0x03
	CRYPTO_ALGOFAM_SHA2_384	0x04
	CRYPTO_ALGOFAM_SHA2_512	0x05
	CRYPTO_ALGOFAM_SHA2_512_224	0x06
	CRYPTO_ALGOFAM_SHA2_512_256	0x07
	CRYPTO_ALGOFAM_SHA3_224	0x08
	CRYPTO_ALGOFAM_SHA3_256	0x09
	CRYPTO_ALGOFAM_SHA3_384	0x0A
	CRYPTO_ALGOFAM_SHA3_512	0x0B
	CRYPTO_ALGOFAM_SHAKE128	0x0C
	CRYPTO_ALGOFAM_SHAKE256	0x0D
	CRYPTO_ALGOFAM_SIPHASH	0x1C
<b>Post-Build Variant Value</b>	false	
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X All Variants
	<b>Link time</b>	--
	<b>Post-build time</b>	--
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X All Variants
	<b>Link time</b>	--
	<b>Post-build time</b>	--
<b>Scope / Dependency</b>	scope: local	

<b>SWS Item</b>	<b>ECUC_Crypto_00036 :</b>	
<b>Name</b>	CryptoPrimitiveAlgorithmMode	
<b>Parent Container</b>	CryptoPrimitive	
<b>Description</b>	Determines the algorithm mode used for the crypto service	
<b>Multiplicity</b>	1	
<b>Type</b>	EcucEnumerationParamDef	
<b>Range</b>	CRYPTO_ALGOMODE_12ROUNDS	0x0D
	CRYPTO_ALGOMODE_20ROUNDS	0x0E
	CRYPTO_ALGOMODE_8ROUNDS	0x0C
	CRYPTO_ALGOMODE_CBC	0x02

	CRYPTO_ALGOMODE_CFB	0x03
	CRYPTO_ALGOMODE_CMAC	0x10
	CRYPTO_ALGOMODE_CTR	0x05
	CRYPTO_ALGOMODE_CTRDRBG	0x12
	CRYPTO_ALGOMODE_CUSTOM	0xFF
	CRYPTO_ALGOMODE_ECB	0x01
	CRYPTO_ALGOMODE_GCM	0x06
	CRYPTO_ALGOMODE_GMAC	0x11
	CRYPTO_ALGOMODE_HMAC	0x0F
	CRYPTO_ALGOMODE_NOT_SET	0x00
	CRYPTO_ALGOMODE_OFB	0x04
	CRYPTO_ALGOMODE_PXXXR	0x09
	CRYPTO_ALGOMODE_RSAES_OAEP	0x08
	CRYPTO_ALGOMODE_RSAES_PKCS1_v1_5	0x09
	CRYPTO_ALGOMODE_RSASSA_PKCS1_v1_5	0x0B
	CRYPTO_ALGOMODE_RSASSA_PSS	0x0A
	CRYPTO_ALGOMODE_SIPHASH_2_4	0x13
	CRYPTO_ALGOMODE_SIPHASH_4_8	0x14
	CRYPTO_ALGOMODE_XTS	0x07
<b>Post-Build Variant Value</b>	false	
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X All Variants
	<b>Link time</b>	--
	<b>Post-build time</b>	--
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X All Variants
	<b>Link time</b>	--
	<b>Post-build time</b>	--
<b>Scope / Dependency</b>	scope: local	

<b>SWS Item</b>	<b>ECUC_Crypto_00037 :</b>	
<b>Name</b>	CryptoPrimitiveAlgorithmSecondaryFamily	
<b>Parent Container</b>	CryptoPrimitive	
<b>Description</b>	Determines the algorithm secondary family used for the crypto service	
<b>Multiplicity</b>	1	
<b>Type</b>	EcucEnumerationParamDef	
<b>Range</b>	CRYPTO_ALGOFAM_3DES	0x13
	CRYPTO_ALGOFAM_AES	0x14
	CRYPTO_ALGOFAM_BLAKE_1_256	0x0F
	CRYPTO_ALGOFAM_BLAKE_1_512	0x10
	CRYPTO_ALGOFAM_BLAKE_2s_256	0x11
	CRYPTO_ALGOFAM_BLAKE_2s_512	0x12
	CRYPTO_ALGOFAM_BRAINPOOL	0x18
	CRYPTO_ALGOFAM_CHACHA	0x15
	CRYPTO_ALGOFAM_CUSTOM	0xFF
	CRYPTO_ALGOFAM_DRBG	0x20
	CRYPTO_ALGOFAM_ECCANSI	0x1e
	CRYPTO_ALGOFAM_ECCNIST	0x19
	CRYPTO_ALGOFAM_ECCSEC	0x1f
	CRYPTO_ALGOFAM_ED25519	0x17
	CRYPTO_ALGOFAM_FIPS186	0x21
	CRYPTO_ALGOFAM_NOT_SET	0x00
	CRYPTO_ALGOFAM_PADDING_ONEWITHZEROS	0x23
	CRYPTO_ALGOFAM_PADDING_PKCS7	0x22
	CRYPTO_ALGOFAM_RIPEMD160	0x0E
	CRYPTO_ALGOFAM_RNG	0x1B

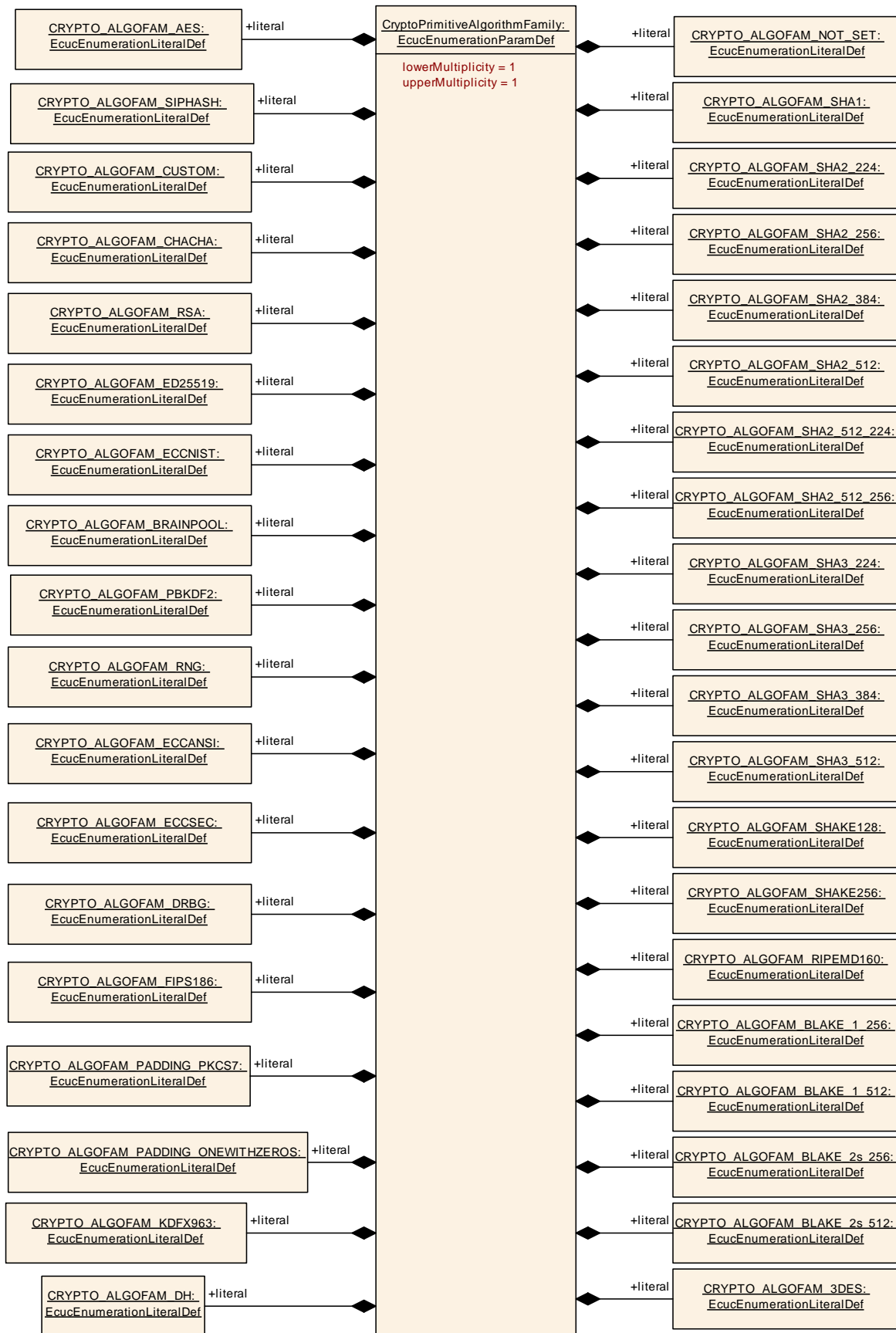


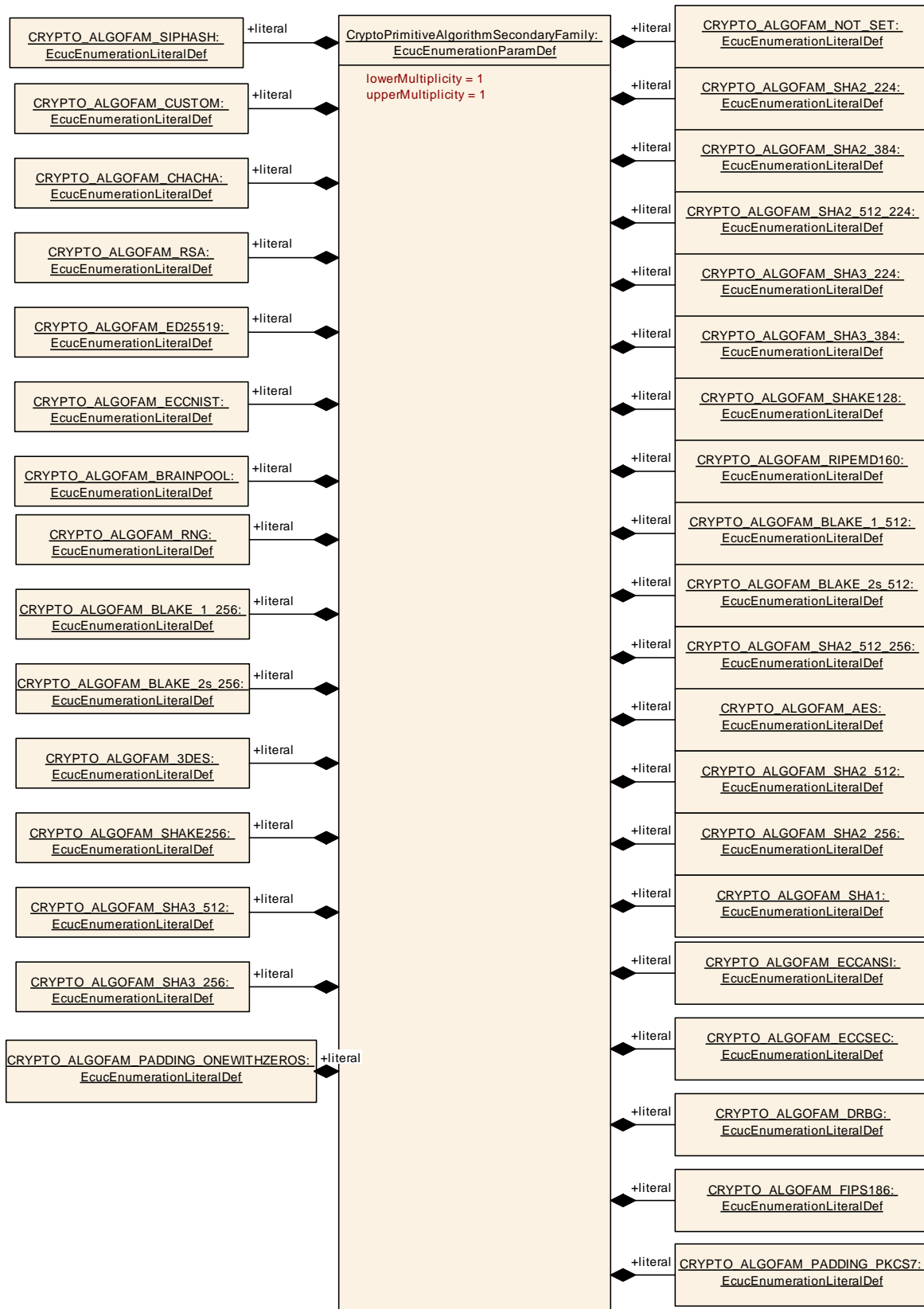
	CRYPTO_ALGOFAM_RSA	0x16
	CRYPTO_ALGOFAM_SHA1	0x01
	CRYPTO_ALGOFAM_SHA2_224	0x02
	CRYPTO_ALGOFAM_SHA2_256	0x03
	CRYPTO_ALGOFAM_SHA2_384	0x04
	CRYPTO_ALGOFAM_SHA2_512	0x05
	CRYPTO_ALGOFAM_SHA2_512_224	0x06
	CRYPTO_ALGOFAM_SHA2_512_256	0x07
	CRYPTO_ALGOFAM_SHA3_224	0x08
	CRYPTO_ALGOFAM_SHA3_256	0x09
	CRYPTO_ALGOFAM_SHA3_384	0x0A
	CRYPTO_ALGOFAM_SHA3_512	0x0B
	CRYPTO_ALGOFAM_SHAKE128	0x0C
	CRYPTO_ALGOFAM_SHAKE256	0x0D
	CRYPTO_ALGOFAM_SIPHASH	0x1C
<b>Post-Build Variant Value</b>	false	
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X All Variants
	<b>Link time</b>	--
	<b>Post-build time</b>	--
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X All Variants
	<b>Link time</b>	--
	<b>Post-build time</b>	--
<b>Scope / Dependency</b>	scope: local	

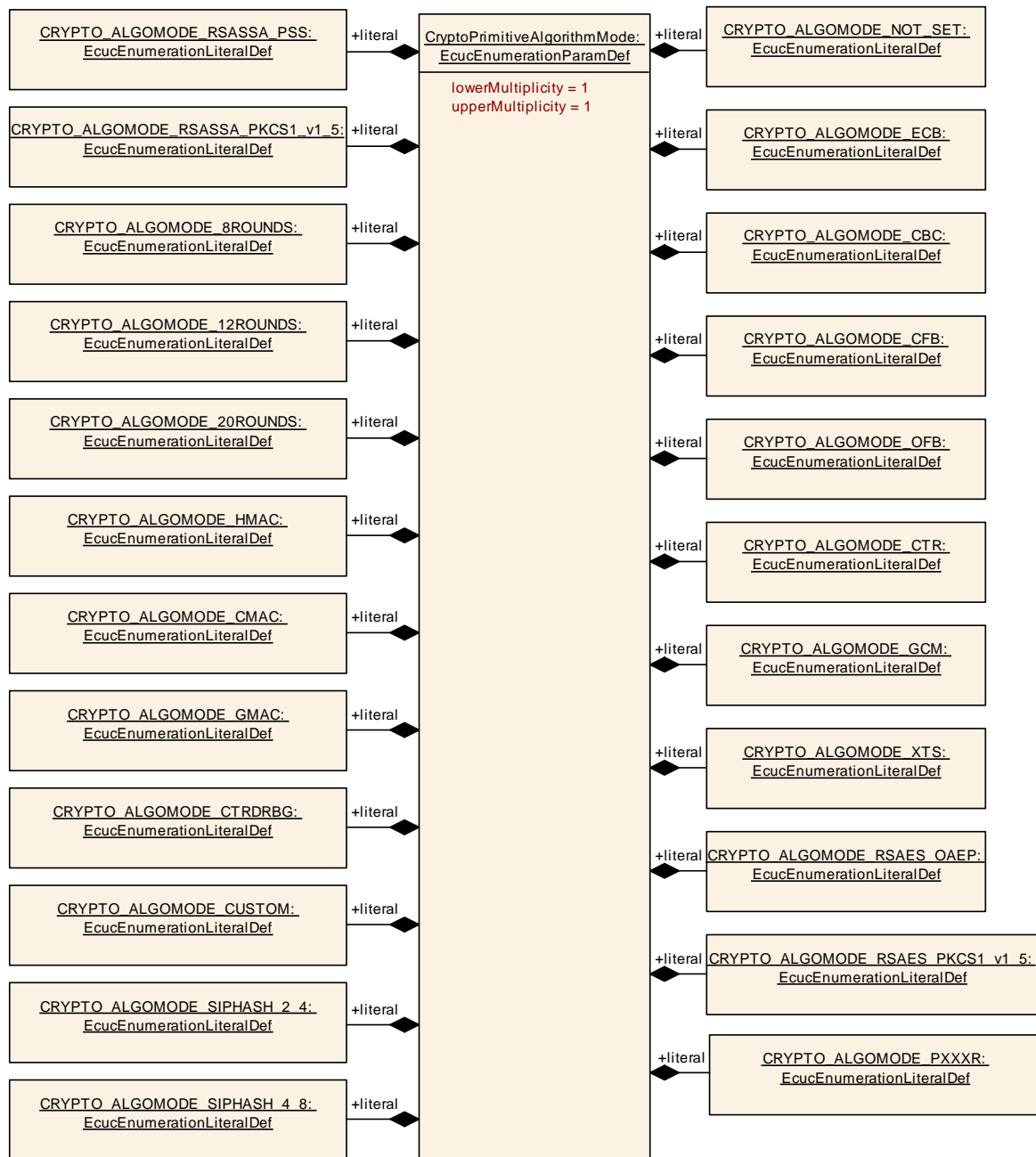
<b>SWS Item</b>	<b>ECUC_Crypto_00034 :</b>	
<b>Name</b>	CryptoPrimitiveService	
<b>Parent Container</b>	CryptoPrimitive	
<b>Description</b>	Determines the crypto service used for defining the capabilities	
<b>Multiplicity</b>	1	
<b>Type</b>	EcucEnumerationParamDef	
<b>Range</b>	AEAD_DECRYPT	0x8
	AEAD_ENCRYPT	0x7
	DECRYPT	0x6
	ENCRYPT	0x5
	HASH	0x9
	MAC_GENERATE	0x2
	MAC_VERIFY	0x1
	RANDOM	0xA
	SIGNATURE_GENERATE	0x4
	SIGNATURE_VERIFY	0x3
<b>Multiplicity Configuration Class</b>	<b>Pre-compile time</b>	X All Variants
	<b>Link time</b>	--
	<b>Post-build time</b>	--
<b>Value Configuration Class</b>	<b>Pre-compile time</b>	X All Variants
	<b>Link time</b>	--
	<b>Post-build time</b>	--
<b>Scope / Dependency</b>	scope: local	

**No Included Containers**









## 10.2 Published Information

Published information contains data defined by the implementer of the SW module that does not change when the module is adapted (i.e. configured) to the actual HW/SW environment. It thus contains version and manufacturer information.

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