Document Title	Requirements on Secure Onboard Communication
Document Owner	AUTOSAR
Document Responsibility	AUTOSAR
Document Identification No	653

Document Status	Final
Part of AUTOSAR Standard	Classic Platform
Part of Standard Release	4.3.1

Document Change History

Date	Release	Changed by	Change Description
2017-12-08	4.3.1	AUTOSAR Release Management	• Minor corrections / clarifications / editorial changes; For details please refer to the Change Documentation.
2016-11-30	4.3.0	AUTOSAR Release Management	• Minor corrections / clarifications / editorial changes; For details please refer to the ChangeDocumentation
2015-07-31	4.2.2	AUTOSAR Release Management	• Minor corrections / clarifications / editorial changes; For details please refer to the ChangeDocumentation
2014-10-31	4.2.1	AUTOSAR Release Management	• Initial Release

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 Scope of Document

This document lists the requirements applicable to the design of the SecOC module of AUTOSAR.

2 Conventions to be used

- The representation of requirements in AUTOSAR documents follows the table specified in [TPS_STDT_00078].

- In requirements, the following specific semantics shall be used (based on the Internet Engineering Task Force IETF).

  The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as:

  - SHALL: This word means that the definition is an absolute requirement of the specification.
  - SHALL NOT: This phrase means that the definition is an absolute prohibition of the specification.
  - MUST: This word means that the definition is an absolute requirement of the specification due to legal issues.
  - MUST NOT: This phrase means that the definition is an absolute prohibition of the specification due to legal constraints.
  - SHOULD: This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
  - SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
  - MAY: This word, or the adjective „OPTIONAL“, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation, which does not include a particular option, MUST be prepared to interoperate with another implementation, which does include the option, though perhaps with reduced functionality. In the same vein an implementation, which does include a particular option, MUST be prepared to interoperate with another implementation, which does not include the option (except, of course, for the feature the option provides.)

3 Acronyms and abbreviations

Acronyms and abbreviations that have a local scope are not contained in the AUTOSAR glossary.

Acronym:	Description:
MAC	Message Authentication Code
SecOC	Secure Onboard Communication
Abbreviation	**Description:**
NVM	Non volatile memory
Authentic I-PDU	An Authentic I-PDU is an arbitrary AUTOSAR I-PDU that is completely secured during network transmission by means of the Secured I-PDU
Secured I-PDU	A Secured I-PDU is an AUTOSAR I-PDU that contains Payload of an Authentic I-PDU supplemented by additional Authentication Information.

4 Requirements Tracing

Requirement	Description	Satisfied by
RS_BRF_01600	AUTOSAR communication shall support time-out handling	SRS_SecOC_00021
RS_BRF_01704	AUTOSAR communication shall support the CAN communication bus	SRS_SecOC_00012
RS_BRF_01712	AUTOSAR communication shall support the adaptable speed offered by CAN FD	SRS_SecOC_00012
RS_BRF_01720	AUTOSAR communication shall support the standardized transport protocol for Diagnostics over CAN	SRS_SecOC_00010
RS_BRF_01728	AUTOSAR communication shall support J1939 transport protocol	SRS_SecOC_00010
RS_BRF_01736	AUTOSAR communication shall support dynamic allocation of addresses as requested by J1939 network management	SRS_SecOC_00010
RS_BRF_01744	AUTOSAR communication shall support TTCAN	SRS_SecOC_00010
RS_BRF_01752	AUTOSAR communication shall support FlexRay	SRS_SecOC_00012
RS_BRF_01760	AUTOSAR communication shall support the standardized transport protocol for Diagnostics on FlexRay	SRS_SecOC_00012
RS_BRF_01768	AUTOSAR communication shall support LIN	SRS_SecOC_00012
RS_BRF_01776	AUTOSAR communication shall support Ethernet	SRS_SecOC_00012
RS_BRF_01784	AUTOSAR communication shall support the IP protocol stack	SRS_SecOC_00010
RS_BRF_02035	AUTOSAR shall support Message Data Authentication	SRS_SecOC_00001, SRS_SecOC_00002, SRS_SecOC_00003, SRS_SecOC_00005, SRS_SecOC_00006, SRS_SecOC_00007,

		SRS_SecOC_00010, SRS_SecOC_00013, SRS_SecOC_00017, SRS_SecOC_00020, SRS_SecOC_00021, SRS_SecOC_00022, SRS_SecOC_00025, SRS_SecOC_00026, SRS_SecOC_00028, SRS_SecOC_00030
RS_BRF_02036	AUTOSAR shall support Message Data Freshness Verification	SRS_SecOC_00001, SRS_SecOC_00002, SRS_SecOC_00003, SRS_SecOC_00005, SRS_SecOC_00006, SRS_SecOC_00007, SRS_SecOC_00013, SRS_SecOC_00017, SRS_SecOC_00020, SRS_SecOC_00021, SRS_SecOC_00022, SRS_SecOC_00025, SRS_SecOC_00026, SRS_SecOC_00028, SRS_SecOC_00029, SRS_SecOC_00030
RS_BRF_02037	AUTOSAR shall support Message Data Integrity Verification	SRS_SecOC_00001, SRS_SecOC_00002, SRS_SecOC_00003, SRS_SecOC_00005, SRS_SecOC_00006, SRS_SecOC_00007, SRS_SecOC_00013, SRS_SecOC_00017, SRS_SecOC_00020, SRS_SecOC_00021, SRS_SecOC_00022, SRS_SecOC_00025, SRS_SecOC_00026, SRS_SecOC_00028, SRS_SecOC_00030
RS_BRF_02200	AUTOSAR diagnostic shall provide external access to internal configuration and calibration data	SRS_SecOC_00001, SRS_SecOC_00002, SRS_SecOC_00003, SRS_SecOC_00005, SRS_SecOC_00006

5 Template for Requirements Specific

5.1 Template for Requirements Specification

The requirement structure is defined in TPS_StdT_00077.

5.2 Functional Overview

The purpose of the secure on-board Communication (SecOC) module is to provide an AUTOSAR BSW Module to transmit secured data between two or more peers exchanging information over an automotive embedded network.

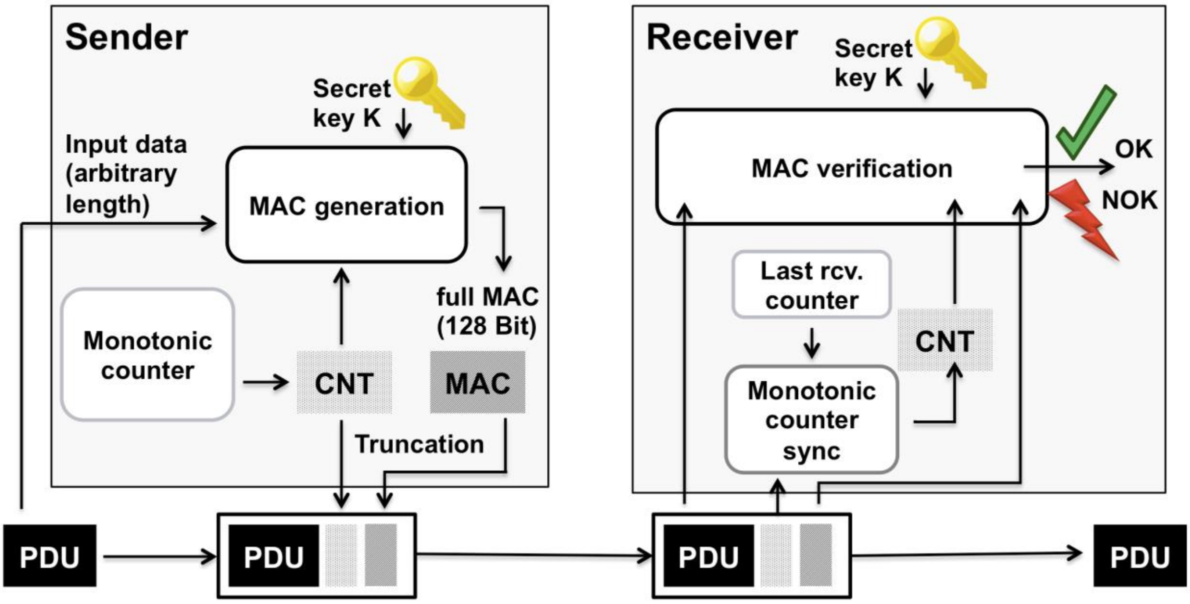

Figure 1: Message Authentication and Freshness Verification

6 Requirement Specification

6.1 Functional Requirements

6.1.1 Configuration

6.1.1.1 [SRS_SecOC_00001] Selection of Authentic I-PDU ⌈

Type:	Valid
Description:	It shall be configurable, which Authentic I-PDU is to be secured.
Rationale:	It is necessary to be able to select and configure the Authentic I-PDUs that need to be secured.
Use Case:	The SecOC configurator selects the PDU IDs that refer to I-PDUs that shall be secured. He/she adds security related configuration data so that a specific level of security is realized.
Dependencies:	[SRS_SecOC_00003]
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037,RS_BRF_02200*)

6.1.1.2 [SRS_SecOC_00002] Range of verification retry by the receiver ⌈

Type:	Valid
Description:	The range of verification retry with self-updated freshness information shall be configurable.
Rationale:	When the receiver is allowed to perform verification retry over a given message with self-updated freshness information, it is necessary to be able to configure the number of retries which are acceptable to match with the desired robustness of the SecOC module.
Use Case:	The security expert and the system designer configure the number of verification retries that are acceptable from a security perspective.
Dependencies:	[SRS_SecOC_00007]
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037,RS_BRF_02200*)

6.1.1.3 [SRS_SecOC_00003] Configuration of different security properties / requirements ⌈

Type:	Valid
Description:	Different security properties shall be configurable.
Rationale:	The assessment may vary in several parameters and its security needs. Thus the level of protection shall be configurable to adapt to these needs by means of a set of adequate parameters.
Use Case:	Security experts define the different security properties. For every message with security protection needs, the appropriate properties may be selected.
Dependencies:	
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037,RS_BRF_02200*)

6.1.2 Initialisation

6.1.2.1 [SRS_SecOC_00005] Initialisation of security information ⌈

Type:	Valid
Description:	The SecOC module's security configuration shall get initialised at module start-up.
Rationale:	The SecOC module needs security configuration information (Key-IDs, Freshness Values) to perform its operations. Therefore, this information shall get recovered and configured before it starts its processing operation.
Use Case:	The SecOC loads the ID of the PDUs, the authorized authentication retry counter and the properties that are used for the processing of its incoming communications from upper and lower layers.
Dependencies:	[SRS_SecOC_00001], [SRS_SecOC_00002], [SRS_SecOC_00003]
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037,RS_BRF_02200*)

6.1.3 Normal operations

[SRS_SecOC_00026] Capability to transmit data and authentication information separately

⌈

Type:	Valid
Description:	SecOC shall support transmitting the Authentic I-PDU and its Authenticator in separate messages.
Rationale:	It may not be possible to secure a message by appending additional data for several reasons, requiring it so be sent separately.
Use Case:	• The data to be authenticated takes up too much space inside the transmitted messages to add an authenticator of acceptable length • A preexisting message needs to be secured for some receivers but for others • A preexisting message needs to be secured but not all receivers can be updated to support the modified message's content
Dependencies:	-
Supporting Material:	-

⌋ (*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037)*

[SRS_SecOC_00028] Properly match up data and authentication information when verifying

⌈

Type:	Valid
Description:	SecOC shall ensure that an Authentic I-PDU is verified using the correct Authenticator when transmitting them in separate messages.
Rationale:	When an Authentic I-PDU and its authenticator are transmitted in separate messages then either message may be lost during transmission. In this case SecOC may match up two non-corresponsing messages and try to verify an Authentic I-PDU with an Authenticator that does not match. This verification will necessarily fail and SecOC may send a verification error to the upper layers. The application layer may categorize this as an attack, even though messages just have been genuinely lost.
Use Case:	If an upper layer is responsible for detecting security attacks based on the information from SecOC then SecOC needs to provide information which is accurate. Message loss should be reported as such independent of the cause (e.g. hardware failure or denial of service).
Dependencies:	**SRS_SecOC_00026**
Supporting	-

Material:	

⌋ (*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037*)

6.1.3.1 [SRS_SecOC_00006] Creation of a Secured I-PDU from an Authentic I-PDU

⌈

Type:	Valid
Description:	The security information (MAC and Freshness Counter) shall be communicated together with the authentic I-PDU and result in a secured I-PDU that can be transmitted in an L-PDU or an N-PDU depending on the protocol capabilities.
Rationale:	In order for a receiver to verify a message came from a trusted sender and has not been intentionally modified, it is necessary that the SecOC module of a sender is capable of communicating verification information together with the information which it has to be secured. The sender and the receiver SecOC module shall be able to process the message together with its additional security information (MAC and freshness counter) to perform the verification process before providing the secured PDU to other software layers.
Use Case:	An authentic I-PDU is configured as secured by the SecOC configuration developer. When it is processed by the SecOC module, security information is added to create a secured I-PDU.
Dependencies:	[SRS_SecOC_00001]
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037,RS_BRF_02200*)

6.1.3.2 [SRS_SecOC_00007] Verification retry by the receiver

⌈

Type:	Valid
Description:	Upon verification failure on the received side, the SecOC module shall provide a way to retry verification processing with self-calculated freshness information until verification succeeds with a configurable range.
Rationale:	Loss of synchronization between the sender and the receiver shall not lead to a verification failure when verification attempts remain in a configurable acceptable range. It is therefore necessary to allow the receiver of a secured message to reattempt verification with self-updated freshness information until the maximum number of configured reattempts is reached.
Use Case:	When the verification of a received Secured I-PDU fails, the same data can be reprocessed by the receiver using different self-calculated freshness information.
Dependencies:	[SRS_SecOC_00002]
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037*)

6.1.3.3 [SRS_SecOC_00010] Communication security is available for all communication paradigms of AUTOSAR

⌈

Type:	Valid
Description:	The concept shall provide mechanisms for secure communication from one source ECU to one or more ECUs.

Rationale:	Some signals may be intended to be used by only one ECU, while others contain values required for different allocated functions.
Use Case:	Example for 1:1: The body control ECU should send a message to the parking brake unit indicating a request to release the break; Example for 1:n: The speed value is required for different functions in the vehicle which may be allocated to different ECUs, such as speedometer, cruise control or navigation system. In both examples, the sink ECU(s) shall be able to verify that the signals were sent by a sufficiently privileged source ECU and are transmitted unmodified. Data verification shall be performed, independently from other possible receivers, by every ECU. Receivers without security requirements shall be able to receive and use the signal data without the need to perform any additional computation.
Dependencies:	
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_01720,RS_BRF_01728,RS_BRF_01736, RS_BRF_01744,RS_BRF_01784*)

6.1.3.4 [SRS_SecOC_00029] Flexible freshness construction

⌈

Type	Valid
Description:	The generation of freshness for an Authentic-PDU shall be generated and maintained by an external component. This can be done either by a software component (SW-C) or a complex device driver (CD)
Rationale:	There are different approaches from OEMs to generate freshness. This cannot be described in an AUTOSAR specification nor can be implemented and maintained in an AUTOSAR module. To provide higher flexibility to the freshness, the construction of freshness shall be located in a separate software module.
Use Case:	Provide a flexible way to generated freshness for a secured PDU.
Dependencies:	[SRS_SECOC_00002], [SRS_SECOC_00003], [SRS_SECOC_00005], [SRS_SECOC_00005]
Supporting Material:	

⌋ (*RS_BRF_02036*)

6.1.3.5 [SRS_SecOC_00012] Support of Automotive BUS Systems

⌈

Type:	Valid
Description:	The SecOC module shall be applicable for the different kind of bus systems that are supported by AUTOSAR and that are typical for automotive environments
Rationale:	All bus protocols supported by Autosar shall benefit from the SecOC design
Use Case:	Low bandwidth busses like CAN shall be supported as well as technologies for large data link, like Ethernet.
Dependencies:	
Supporting Material:	

⌋(*RS_BRF_01704,RS_BRF_01712,RS_BRF_01752,RS_BRF_01760, RS_BRF_01768,RS_BRF_01776*)

6.1.3.6 [SRS_SecOC_00030] Support of capability to extract Authentic I-PDU without Authentication

⌈

Type	Valid
Description:	The SecOC module shall be capable to extract Authentic I-PDU from Secured I-PDU, without Authentication.
Rationale:	SecOC can be used as an extractor of Authentic I-PDU from Secured I-PDU, to enable low latency GW behaviour when a part of downstream communication clusters doesn't require authentication of PDUs.
Use Case:	Gateway
Dependencies:	[SRS_SecOC_00025]
Supporting Material:	

⌋ (RS_BRF_02035,RS_BRF_02036, RS_BRF_02037)

6.1.4 Support for end-to-end and point-to-point protection

If data is not directly transmitted over a direct connection or bus system but rather over several hops or via a gateway, there are two modes of protection which both shall be supported by the SecOC module: end-to-end and point-to-point protection. End point of communication is defined by an ECU and not by a SWC.

- Definition of point to point secured communication: In a point-to-point scheme the communications are secured between each single peer of the network transmitting the data, so that in case of multiple hops, an authentication is performed several times (i.e. on each sender of the transmission) path and a verification is performed several times (i.e. on each receiver of the transmission path).
- Definition of end to end secured communication: In an end-to-end scheme the communications are secured between the sender and the receiver(s) regardless of the intermediate hops. Authentication is performed once at the sender side and verification is performed once at the receiver(s) side.

6.1.4.1 [SRS_SecOC_00013] Support for end-to-end and point-to-point protection⌈

Type:	Valid
Description:	Support for end-to-end and point-to-point protection.
Rationale:	While some signals are simply forwarded and no further requirements are given for the channel or relaying entities in between, other may pass through relaying entities that can do changes on the packet content and thus need to be trusted by the receiving entity.
Use Case:	An ECU communicates data that is transmitted over several logical networks with different security properties. A re-authentication gateway bridges the data from a logical network to the other and processes verification and re-authentication.
Dependencies:	
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037*)

6.1.4.2 [SRS_SecOC_00017] PDU security information override ⌈

Type:	Valid
Description:	It shall be possible to override the verification result for PDUs to force verification failure and thus make the SecOC module reject the message.
Rationale:	When an attack has been detected or the system cannot be trusted, the verification result shall be overridden to fail to force their rejection regardless of the received security information as long as the communication channel is not secured.
Use Case:	When a receiver detects an attack or assumes it is not correctly synchronized, it can decide to reject messages as long as it does not trust the communication channel.
Dependencies:	
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037*)

6.1.5 Shutdown Operation

6.1.5.1 [SRS_SecOC_00020] Security operational information persistency⌈

Type:	Valid
Description:	The SecOC module shall provide a secured persistency mechanism in NVM of security information that is used for its normal operation before the shutdown operation is finished.
Rationale:	Security information like freshness counter can be reused when the SecOC module is shutdown to avoid resynchronization of SecOC modules at each restart.
Use Case:	Security information before the shutdown is reused after the restart of the module.
Dependencies:	
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037*)

6.1.6 Fault Operation

6.1.6.1 [SRS_SecOC_00021] Transmitted PDU authentication failure handling ⌈

Type:	Valid
Description:	Upon authentication failure of an authentic I-PDU, the unsecured PDU shall not get sent.
Rationale:	The same functional reactivity that is associated to the transmission failure of a given PDU shall remain applicable to its transmission failure when it is secured. If the SecOC module fails to perform authentication, the PDU shall not be sent. In that case, the reactivity (application) takes into account that communication cannot be performed.
Use Case:	Authentication failure does not result in the transmission of an unsecured message.
Dependencies:	
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037,RS_BRF_01600*)

6.1.6.2 [SRS_SecOC_00022] Received PDU verification failure handling⌈

Type:	Valid

Description:	Upon verification failure of a received secured PDU, the authentic PDU shall not get propagated to any other module and a notification shall be provided.
Rationale:	Signal data contained in a secured PDU which resulted in failed verification shall not be used for further processing since the signal data is considered to be manipulated.
Use Case:	A SWC triggers some failsafe mode when it is notified that the information it is supposed to receive cannot be considered.
Dependencies:	
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037*)

6.2 Non-Functional Requirements (Qualities)

6.2.1 Timing Requirements

6.2.1.1 [SRS_SecOC_00025] Authentication and verification processing time ⌈

Type:	Valid
Description:	Authentication and verification processing shall be performed in a timely fashion so that the real time critical signals do not get affected.
Rationale:	Transmission and reception of time critical signals between the running applications of two or more peers shall not get penalised by the additional processing of their underlying communication software layers such that the signals are finally rejected. It is necessary that when time critical signals transmitted and received through a Secured I-PDU, the additional processing required by the SecOC module remains under a value that is predictable and compatible with the time constraints of the concerned signals.
Use Case:	A legitimate authenticated message is verified and passed to the receiving SWC within the expected timeframe without experiencing signal monitoring errors.
Dependencies:	[SRS_SecOC_00014]
Supporting Material:	

⌋(*RS_BRF_02035,RS_BRF_02036,RS_BRF_02037*)

7 References

7.1 Deliverables of AUTOSAR

[DOC_LayeredSoftwareArchitecture]
Layered Sofware Architecture
AUTOSAR_EXP_LayeredSoftwareArchitecture.pdf

[DOC_COM_TYPES]
Specification of Communication Stack Types
AUTOSAR_SWS_CommunicationStackTypes.pdf

[DOC_VFB]
Specification of the Virtual Functional Bus
AUTOSAR_EXP_VFB.pdf

[DOC_ECUC]
Specification of ECU Configuration
AUTOSAR_TPS_ECUConfiguration.pdf

[DOC_SWS_COM]
Specification of Communication
AUTOSAR_SWS_COM.pdf

[DOC_SWS_LDCOM]
Specification of Large Data COM
AUTOSAR_SWS_LargeDataCOM.pdf

[DOC_TR_Glossary]
Glossary
AUTOSAR_TR_Glossary.pdf

[DOC_RS_Features]
Requirements on AUTOSAR Features
AUTOSAR_RS_Features.pdf

[DOC_SWS_CryptoServiceManager]
Specification of Crypto Service Manager
AUTOSAR_SWS_CryptoServiceManager

[DOC_TPS_STDT]
Standardization Template
AUTOSAR_TPS_StandardizationTemplate.pdf

7.2 Related standards and norms

[DOC_IEC7498-1] The Basic Model, IEC Norm, 1994

[DOC_FIPS-180-4] National Institute of Standards and Technology (NIST): FIPS-180-4, Secure Hash Standard (SHS), March 2012
http://csrc.nist.gov/publications/fips/fips180-4

[DOC_FIPS-197] Advanced Encryption Standard (AES), U.S. Department of Commerce, Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA, Federal Information Processing Standards Publication, 2001
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf