



SURFACE VEHICLE INFORMATION REPORT

J3101™-1

JUL2024

Issued

2024-07

Hardware Protected Security Environment - Application Programming Interface Analysis - Information Report

RATIONALE

The purpose of this information report is to provide an analysis and summary of the coverage of SAE J3101 requirements by existing Application Programming Interfaces (APIs). The report aims to identify areas of coverage within these APIs and to highlight any gaps in coverage that need to be addressed. By examining the current state of API support for SAE J3101 devices, this report will help to inform and guide future development efforts in this area.

TABLE OF CONTENTS

1.	SCOPE.....	2
2.	REFERENCES.....	2
2.1	Applicable Documents.....	2
3.	METHODOLOGY.....	2
3.1	Requirements Categorization.....	2
3.2	Assessed API Specification.....	3
3.3	API Analysis.....	3
3.4	Interpreting Coverage Analysis.....	3
4.	AUTOSAR CLASSIC PLATFORM CRYPTO API ANALYSIS.....	4
4.1	Overview.....	4
4.2	API Impacted Requirements - AUTOSAR Crypto API Analysis.....	5
4.3	API Required Requirements - AUTOSAR Crypto API Analysis.....	8
4.4	API Implementation Specific Requirements.....	10
5.	NOTES.....	12
5.1	Revision Indicator.....	12
APPENDIX A	SAE J3101 REQUIREMENTS CLASSIFIED OUT OF SCOPE OF THE API.....	13
Figure 1	Crypto API results.....	4
Table 1	SAE J3101 requirement categories.....	3
Table 2	Coverage analysis categories.....	3
Table 3	API impacted requirements.....	5
Table 4	Requirements with HPSE-specific API.....	8
Table 5	API implementation-specific requirements.....	10

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2024 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, or used for text and data mining, AI training, or similar technologies, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3101-1_202407

For more information on this standard, visit https://www.sae.org/standards/content/J3101-1_202407/

Documents



Standard, visit Sharing Hub

1. SCOPE

To gain an understanding of the software Application Programming Interface (API) landscape for SAE J3101 [SAEJ3101] devices, the SAE Vehicle Electrical Hardware Security Task Force conducted an analysis of various automotive-relevant crypto APIs. The purpose of this analysis was to identify how well the existing APIs cover the SAE J3101 requirements and to highlight the areas of coverage within these APIs. By examining these APIs, the Task Force aimed to gain insights into the current state of API support for SAE J3101 devices and identify any gaps in coverage that need to be addressed.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this specification to the extent specified herein. Unless otherwise indicated, the latest issue of SAE publications shall apply.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE J3101 Hardware Protected Security for Ground Vehicles

2.1.2 ISO Publications

Copies of these documents are available online at <https://webstore.ansi.org/>.

ISO/IEC 19790:2012 Information Technology - Security Techniques - Security Requirements for Cryptographic Modules

2.1.3 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

NIST SP 800-57 Recommendation for Key Management, Part 1: General (January 2016)

NIST FIPS 140-2 Security Requirements for Cryptographic Modules (May 2001)

2.1.4 Other Publications

AUTOSAR Classic Platform Crypto API Version R21-11 (2021). https://www.autosar.org/fileadmin/standards/classic/21-11/AUTOSAR_SWS_CryptoDriver.pdf.

Blake-Wilson, S. and Menezes, A. (1999). Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol. *Lecture Notes in Computer Science*, Springer, 154-170.

3. METHODOLOGY

3.1 Requirements Categorization

All SAE J3101 requirements were extracted into a tabular database for analysis. Requirements were categorized into four categories related to software API: API Required, API Impacted, Implementation Specific, and Internal.

Table 1 - SAE J3101 requirement categories

Category	Description
API Required	This requirement requires a dedicated API to support.
API Impacted	This requirement impacts API design choices but does not itself require an API to fulfill this requirement.
Implementation Specific	This requirement could be supported within an API; however, it may be specific to an individual implementation of an HPSE or API design. The distinction between “API Impacted” is an HPSE firmware implementer may be able to fulfill this requirement without a dedicated API, where “API Impacted” will always influence API design.
Internal	This is a requirement internal to the HPSE firmware or hardware. No external API is required.

Each SAE J3101 requirement was assigned into one of the defined categories.

3.2 Assessed API Specification

The assessed API specification was chosen as it was the latest version available at the time of the analysis. However, it's important to note that newer versions of the API may have changes in coverage when compared to the SAE J3101 requirements. Therefore, it's crucial to keep in mind the potential for differences in coverage when considering newer versions of the API and SAE J3101.

3.3 API Analysis

The committee working group analyzed each SAE J3101 requirement against the assessed specification categorizing the API coverage into the following three categories: Yes, Partial, and No. The categories are described in Table 2.

Table 2 - Coverage analysis categories

Analysis Result	Description
Yes	This SAE J3101 requirement is fulfilled by the assessed specification.
Partial	This SAE J3101 requirement is partially fulfilled by the assessed specification. The details of this choice are included in the comments section for each requirement.
No	This SAE J3101 requirement is not fulfilled by the assessed specification.

3.4 Interpreting Coverage Analysis

This document aims to provide an overview of the coverage of the API under analysis in relation to the SAE J3101 requirements that necessitate the API. The purpose is to identify the requirements that are currently covered and to identify any gaps that require additional support or may be covered by another API. While it is relatively straightforward to determine whether a requirement is covered by the API under analysis, some questions remain regarding the requirements that are either partially covered or not covered at all. Therefore, this document aims to shed light on these outstanding questions to provide a more comprehensive understanding of the API coverage.

What is a reader expected to do regarding non-covered requirements? What is a reader expected to do regarding partially covered requirements? In the case of non-covered requirements, the report intends to give practical guidance on why the requirement was deemed non-covered. For example, REQ_6.2.3.7_100 was deemed not covered with the comment that “Device life cycle is out of scope of the AUTOSAR [crypto] API. To implement a device life cycle, additional logic is needed.” In the case of partially covered results, an effort is taken to describe the covered (or non-covered) parts of the requirement.

4. AUTOSAR CLASSIC PLATFORM CRYPTO API ANALYSIS

4.1 Overview

After analyzing 159 SAE J3101 HPSE requirements, it was found that 94 requirements were internal and did not have any effect on the software API for accessing the HPSE, whereas 25 requirements required dedicated API support. The remaining 40 requirements were found to have an impact or implementation-specific dependency on the API. Among these, the analysis revealed that the AUTOSAR Classic Platform Crypto API Version R21-11 covered or partially covered 39 out of the 65 requirements that either do or could impact the HPSE API, resulting in approximately 60% coverage of the SAE J3101 requirements. However, it's worth noting that this analysis only reviewed the Crypto API specification, and some SAE J3101 requirements may be covered by other AUTOSAR layers. Finally, as part of the analysis, two SAE J3101 requirements were identified that are ambiguous and may require refactoring in future SAE J3101 versions. These requirements were flagged “Needs Evaluation” in the analysis.

AUTOSAR Classic Platform Crypto API Results

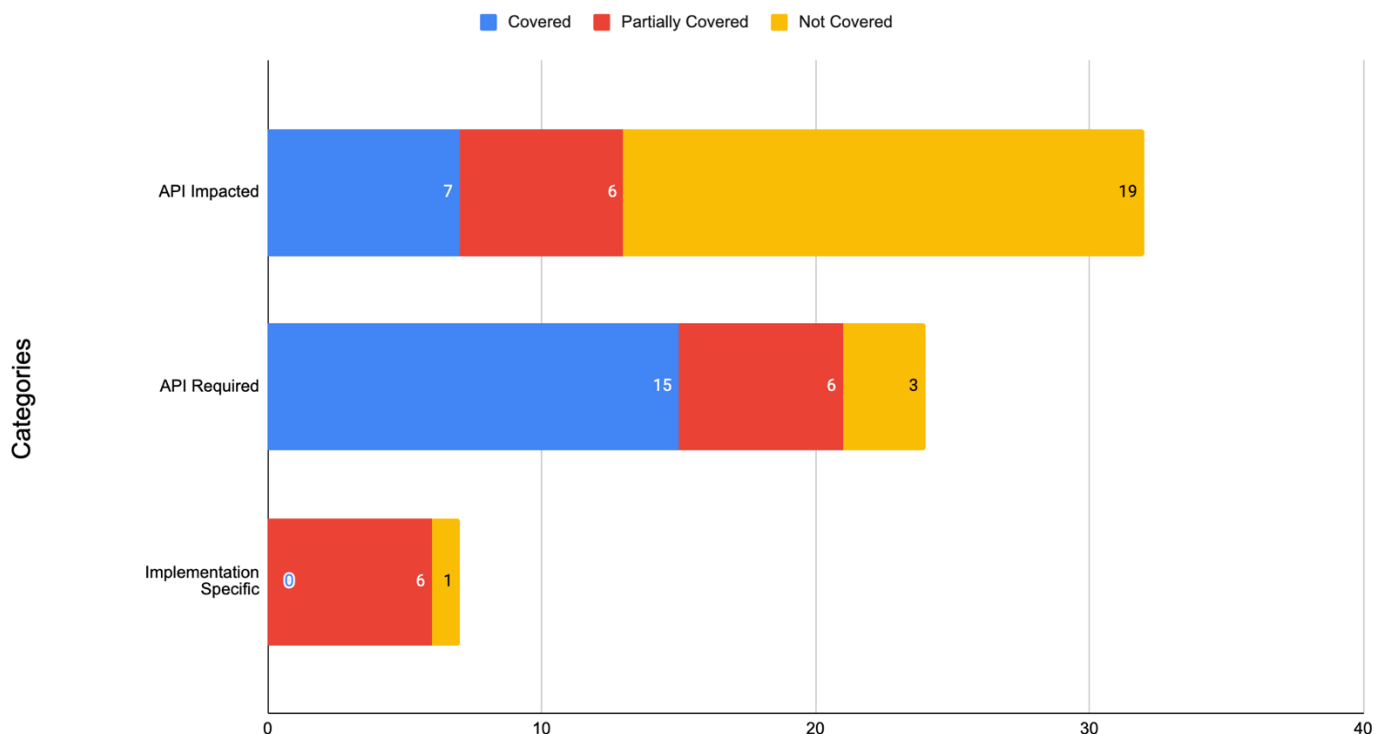


Figure 1 - Crypto API results

4.2 API Impacted Requirements - AUTOSAR Crypto API Analysis

Table 3 - API impacted requirements

Requirement ID	Condition	Section	Subsection	Requirement Description	AUTOSAR Classic Crypto API R21-11	AUTOSAR Crypto API Comment
REQ_6.2.3.3_10	[MANDATORY]	Cryptographic Key Protection	Protection at Use	If all verifications/authorizations passed successfully, the hardware protected security environment shall perform all cryptographic operations within the hardware protected security environment and return only the resulting data to the normal environment.	Yes	
REQ_6.2.3.4_10	[MANDATORY]	Cryptographic Key Protection	Key Ownership and Accessibility	The hardware protected security environment shall not allow access to any keys stored internally outside of the hardware protected security environment, except in an encrypted form, with explicit authorization from the hardware protected security environment.	Yes	Allows fulfilling requirements through configuring the CRYPTO_RA_ENCRYPTED key flag. Must be configured properly.
REQ_6.2.3.4.2_70	[OPTIONAL]	Cryptographic Key Protection	Key Access Control	The hardware protected security environment shall require explicit authorization to export any keys to an authenticated and authorized user.	No	Fine grain user access control is not part of the AUTOSAR API.
REQ_6.2.3.4.3_40	[MANDATORY]	Cryptographic Key Protection	Key Access Policies	The hardware protected security environment shall manage key attributes to protect a key from use by an inappropriate function or algorithm (e.g., signature key use in an encryption algorithm).	Yes	
REQ_6.2.3.4.4_30	[MANDATORY]	Cryptographic Key Protection	Key Access Policies	The hardware protected security environment shall implement access control for each key stored within its hardware protected security environment.	Yes	Access control is only for a single user in AUTOSAR.
REQ_6.2.3.4.4_40	[MANDATORY]	Cryptographic Key Protection	Key Access Policies	Changes to access policies shall be authenticated within the hardware protected security environment as a part of the transaction that requests the changes.	Yes	Support for authenticated key updates using SHE key update protocol.
REQ_6.2.3.7_30	[MANDATORY]	Cryptographic Key Protection	Key Management System	The hardware protected security environment shall perform secure key management in accordance with the principles outlined in NIST SP 800-57. Hardware protected security environment-centric key management objectives should satisfy the requirements provided in NIST FIPS 140-2.	Partial	The API implementation would need to be evaluated for NIST FIPS 140-2. This is implementation specific. Individual algorithms could also be evaluated for CAVP testing.
REQ_6.2.3.7_100	[OPTIONAL]	Cryptographic Key Protection	Key Management System	The hardware protected security environment shall ensure that each transition between life cycle states is cryptographically authenticated by the allowed, designated party.	No	Device life cycle is out of scope of the AUTOSAR API. To implement a device life cycle, additional logic is needed.
REQ_6.2.3.7_120	[MANDATORY]	Cryptographic Key Protection	Key Management System	If the hardware protected security environment requires a common time as an input as a precondition to the security of any key management operation, the authenticity of the time signal and the authorization of its source must be confirmed within the hardware protected security environment before it is valid for use.	No	Secure time is out of scope for AUTOSAR crypto API.
REQ_6.2.3.7.1_10	[OPTIONAL]	Cryptographic Key Protection	Key Management and Provisioning	The hardware protected security environment shall authenticate the key provisioning entity (e.g., by use of a PKI).	No	Certificate management is done outside of the AUTOSAR crypto API.

REQ_6.2.3.7.1_20	[MANDATORY]	Cryptographic Key Protection	Key Management and Provisioning	The hardware protected security environment shall prevent replay and rollback schemes that target an update of a key. For example, such support may include a secure counter or a secure time source, as well as key revocation schemes.	Partial	SHE keys support anti-rollback counters. Key properties allow for keys to be updated or removed.
REQ_6.2.3.7.2_90	[OPTIONAL]	Cryptographic Key Protection	Key Generation	Key generation shall be defined as a local operation to then be distinct from key provisioning or key derivation.	Yes	Separate keygen API interface
REQ_6.2.3.7.4_10	[OPTIONAL]	Cryptographic Key Protection	Key Derivation	The hardware protected security environment shall manage and protect the inputs to a cryptographic key derivation algorithm as a secret key.	Needs Evaluation	This SAE J3101 requirement should only apply to sensitive inputs. There may be inputs that don't require confidentiality. API does cover key derivation.
REQ_6.4.2.1_10	[MANDATORY]	Random Number Generation	Hash-Based DRBG Algorithms	If a DRBG is supported by the hardware protected security environment, then the hardware protected security environment shall support at least one of the following algorithms described below: hash DRBG, HMAC DRBG, or CTR DRBG.	Partial	AUTOSAR doesn't specify what DRBG implementation to use. RNG API is available
REQ_6.4.2.2_10	[MANDATORY]	Random Number Generation	Flooding Protection	The hardware protected security environment shall protect the RNG from a flooding attack, such that the RNG always returns a random number or rejects the request.	Yes	AUTOSAR negative response for CRYPTO_E_RE_ENTROPY_EXHAUSTED supported.
REQ_6.5.3_10	[OPTIONAL]	Nonvolatile Critical Security Parameters	Implementation Considerations	The hardware protected security environment shall support sharing of the values of protected critical security parameters with the normal environment if appropriate, but applications running in the normal environment shall not have the authorization to modify critical security parameters stored within the hardware protected security environment.	Partial	Some limited API access to read parameters within crypto API.
REQ_6.6.2.2_10	[MANDATORY]	Cryptographic Algorithm Agility	Firmware Update	The hardware protected security environment should support secure firmware flashing of itself according to a minimum set of acceptable requirements in order to achieve cryptographic algorithm agility.	No	Not in scope of AUTOSAR Crypto Driver API
REQ_6.6.2.2_25	[MANDATORY]	Cryptographic Algorithm Agility	Firmware Update	Re-flashing of hardware protected security environment should utilize existing secure objects such as secret keys.	No	Not in scope of AUTOSAR Crypto Driver API
REQ_6.6.2.2_30	[MANDATORY]	Cryptographic Algorithm Agility	Firmware Update	The hardware protected security environment shall support personalization of the module (e.g., reprovisioning/reconfiguring of the secure support, including type and number of keys).	No	Not in scope of AUTOSAR Crypto Driver API
REQ_6.6.2.2_50	[MANDATORY]	Cryptographic Algorithm Agility	Firmware Update	The hardware protected security environment should disable deprecated algorithms.	Partial	AUTOSAR API doesn't force deprecation of algorithms; could be deprecated by firmware suppliers.
REQ_6.7.2.2_05	[MANDATORY]	Interface Control	Authorized Access	If a chipset interface access is specified to be securely controlled, then the hardware protected security environment shall authenticate access to that interface only using resources within the hardware protected security environment.	No	Not in scope of AUTOSAR Crypto Driver API
REQ_6.7.2.2_30	[OPTIONAL]	Interface Control	Authorized Access	The hardware protected security environment should implement controlled interface access request authorization separately from firmware authentication.	No	Not in scope of AUTOSAR Crypto Driver API
REQ_6.7.2.2_50	[MANDATORY]	Interface Control	Authorized Access	The hardware protected security environment shall support the use of ECU-specific authentication.	No	Not in scope of AUTOSAR Crypto Driver API. Assumed supported in HPSE firmware, but not explicitly in crypto driver API.