



SURFACE VEHICLE INFORMATION REPORT

J3101™-2

NOV2025

Issued

2025-11

Hardware Protected Security Environment –
Trusted Application Isolation Security Models

RATIONALE

A vehicle could contain two types of Trusted Applications (TAs) for deployment within a Hardware Protected Security Environment (HPSE): TAs developed by the OEM and TAs developed by third-party suppliers. The TAs may require varying strength of isolation mechanisms depending on the source of TAs within the HPSE. We build on SAE J3101 requirements for sandboxing of TAs and secure communication between TAs by providing stakeholders with more technical guidance on sandboxing security model mechanisms. This information report is required to support the TA security requirements within SAE J3101.

INTRODUCTION

The HPSE establishes a hardware root of trust and hardware-based security primitives to provide trust and resilience in vehicle computer system. The HPSE security is proportional to the trusted computing base (TCB) of the HPSE implementation and its internal execution environment. The TCB as defined by NIST^[NISTTCB]: “Totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination responsible for enforcing a security policy.” The HPSE has been designed to contain a minimal TCB to provide the hardware security building blocks specified in SAE J3101. TAs are also part of the HPSE TCB as they are deployed and executed within the HPSE environment. OEMs must carefully balance the risk of increasing the HPSE TCB by introducing multiple TAs from different trusted sources (referred to from hereafter as TA Multitenancy) within the sandbox effectiveness within the HPSE.

TA Multitenancy in the context of an automotive HPSE refers to the ability to deploy TAs from multiple vendors into a trusted HPSE environment. Multitenancy implies the TA owner inherently trusts the HPSE. Increasing the number of TAs within the HPSE increases the TCB and the attack surface; therefore, a separate risk profile must be considered for TAs developed by the OEM and TAs from third-party suppliers. For a secure HPSE deployment with TA multitenancy, isolation building blocks must be defined to provide an effective sandbox model so that these TAs can execute within their own trust domain to prevent compromise of the HPSE.

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 © 2025 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: 1-877-606-7323 (U.S. and Canada only)
Tel: 1-724-776-4970 (outside U.S. and Canada)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE J3101-2_202511

For more information on this standard, visit https://www.sae.org/standards/content/J3101-2_202511/

Documents



Standard, visit Sharing Hub

TABLE OF CONTENTS

1.	SCOPE.....	3
1.1	Objective	3
1.2	Audience	3
2.	REFERENCES.....	4
2.1	Applicable Documents	4
2.1.1	SAE Publications.....	4
2.1.2	ISO/SAE Publications	4
2.1.3	Other Publications.....	4
3.	DEFINITIONS	6
4.	SAE INFORMATION REPORTS MAPPING.....	7
4.1	Management of Confidential Data	7
4.2	Side Channel Attacks Resistance.....	7
4.3	Application Programming Interface Analysis	7
4.4	Global Platform Technologies.....	7
5.	TA ISOLATION	8
5.1	TA Isolation Security Requirements.....	8
5.1.1	Automotive	8
5.1.2	Mobile Phone	9
5.2	HPSE TA Structure and Deployment Model Levels	9
5.3	HPSE Trusted Application Use Cases.....	11
5.4	TA Risk Profile and Governance.....	11
5.5	TA Lifecycle Management	12
5.6	HPSE TA Isolation Building Blocks for Manufacturers	13
5.6.1	HPSE Boundary Trust Domain	15
5.6.2	Trusted OS Trust Domain	16
5.6.3	Partition Trust Domain	17
5.6.4	Software Defined Hardware Isolation Trust Domains.....	18
5.6.5	ECU Core Isolation Trust Domain.....	19
6.	THREAT ANALYSIS TO DETERMINE THE EFFECTIVENESS OF ISOLATION	
	SECURITY MODELS.....	20
6.1	HPSE TA Adversary Model.....	20
6.2	HPSE TA Isolation Structure Pattern Evaluation	21
7.	Recommendations for Securely isolating TAs	23
8.	NOTES.....	23
8.1	Revision Indicator.....	23
Figure 1	SAE J3101 hardware protected security for ground vehicles information reports.....	7
Figure 2	Trust domain isolation levels.....	10
Figure 3	TA lifecycle management architecture.....	12
Figure 4	HPSE boundary trust domain [ARMIsol] [ARMFw]	15
Figure 5	Trusted OS trust domain [ARMIsol] [ARMFw].....	16
Figure 6	Partition trust domain [ARMIsol] [ARMFw] [ARMCCA]	17
Figure 7	Software defined hardware isolation trust domains [Lee2020] [Pinto2020] [Garlati2020].....	18
Figure 8	ECU core isolation trust domain [NISTIR8320] [Brasser2019].....	19
Figure 9	HPSE TAs structure adversarial modeling.....	21
Table 1	SAE J3101 common requirements for TA Isolation.....	8
Table 2	TA isolation structure patterns and deployment model levels.....	14
Table 3	Evaluation criteria for TA isolation	22

1. SCOPE

1.1 Objective

This information report identifies and evaluates isolation building blocks applicable to TA sandboxing within a HPSE. These building blocks can be used to support SAE J3101 TA requirements for sandboxing of TAs and secure communication between TAs. TAs must execute within their own trust domain to prevent compromise of the HPSE and other TAs. TA trust domain isolation strength may vary depending on the risk profile of the TA deployed, hence the requirement for isolation building blocks to match the risk profile. A multitenancy TA HPSE has a higher risk profile than multiple TAs from the same source (e.g., OEM). TA multitenancy must not compromise the security properties of the HPSE (the secure integration and execution of trusted multi-vendor code). In this report, we provide information on the following:

- HPSE TA use cases and risk profiles
- HPSE TA isolation building blocks for manufacturers
- Threat analysis to determine the effectiveness of isolation security models

As the ECU E/E architecture continues to evolve, we must consider the following classification of ECUs and System on Chips (SoCs) for which isolation building blocks apply:

- Application Processor Core(s)
- Realtime Processor Core(s)
- Microcontroller Core(s)

An ECU can be composed of a Normal Environment and Protected Environment (HPSE). Normal Environment is typically separated into user and kernel level privileges, with applications executing at the user privilege level. TAs only execute within the HPSE, and the HPSE is typically divided into user and kernel level privileges which are orthogonal to Normal Environment privileges. The TAs will execute at the same user privilege level within the HPSE; therefore, the isolation building blocks must be implemented at a higher privilege level, such as the HPSE kernel, to ensure that the sandboxing policy can be enforced. The TAs access to HPSE resources is restricted at load time by the sandbox policy which operates at a higher privilege level to the TAs.

This report also differentiates between isolation methods which are applied within the HPSE and isolation methods applied at the ECU level when there is consolidation of ECUs into domain controller or HPC, i.e., isolation abstraction.

1.2 Audience

This information report is written from the perspective of vehicle OEMs and their suppliers of HPSE TAs.

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: 1-877-606-7323 (U.S. and Canada only) or 1-724-776-4970 (outside U.S. and Canada), www.sae.org.

SAE J3101	Hardware Protected Security for Ground Vehicles
SAE J3101-1	Hardware Protected Security Environment - Application Programming Interface Analysis - Information Report
SAE J3101-3	Hardware Protected Security Environment Management of Confidential Data
SAE J3101-5	Hardware Protected Security Environment - GlobalPlatform Technologies Information Report

2.1.2 ISO/SAE Publications

Available from International Organization for Standardization, ISO Central Secretariat, Chemin de Blandonnet 8, CP 401, 1214 Vernier, Geneva, Switzerland, Tel: +41 22 749 01 11, www.iso.org/store.

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

ISO/SAE 21434	Road Vehicles - Cybersecurity Engineering
---------------	---

2.1.3 Other Publications

ARMCCA	ARM, Learn the architecture - Introducing Arm Confidential Compute Architecture Version 3.0 (2023). https://developer.arm.com/documentation/den0125/0300
ARMFW	ARM, Arm Firmware Framework for Armv8-A version 1.0 (2020). https://documentation-service.arm.com/static/5fb7e8a6ca04df4095c1d65e?token=
ARMIsol	ARM, Isolation using virtualization in the Secure world software architecture on Armv8.4 version 1.0 (2018). https://armkeil.blob.core.windows.net/developer/Files/pdf/Isolation%20using%20virtualization%20in%20the%20Secure%20World_Whitepaper.pdf
Brasser2019	Brasser, F., Gens, D., Jauernig, P., Sadeghi, A.-R., and Stapf, E. (2019, February 24-27). <i>SANCTUARY: ARMing TrustZone with user-space enclaves</i> [Conference paper]. 2019 Network and Distributed System Security (NDSS) Symposium (ndss2019), San Diego, CA, USA. https://dx.doi.org/10.14722/ndss.2019.23448 .
Cerdeira2020	Cerdeira, D., Santos, N., Fonseca, P., and Pinto, S. (2020, May 18-21). <i>SoK: Understanding the prevailing security vulnerabilities in TrustZone-assisted TEE systems</i> [Conference paper]. 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA. https://doi.org/10.1109/SP40000.2020.00061 .
DARPA	DARPA. (2024, July 31). <i>Eliminating memory safety vulnerabilities once and for all</i> . https://www.darpa.mil/news/2024/memory-safety-vulnerabilities

Garlati2020	Garlati, C., and Pinto, S. (2020). <i>A clean slate approach to Linux security RISC-V enclaves</i> [Conference paper]. Embedded World Conference 2020, Nuremberg, Germany. https://www.researchgate.net/publication/339784918_A_Clean_Slate_Approach_to_Linux_Security_RISC-V_Enclaves .
GPD_SPE_009	TEE System Architecture v1.3 – GPD_SPE_009 (2022)
GPD_SPE_021	TEE Protection Profile v1.3 – GPD_SPE_021 (2020)
GPD_SPE_123	TEE Management Framework: Open Trust Protocol (OTrP) Profile v1.1 – GPD_SPE_123 (2020)
Lee2020	Lee, D., Kohlbrenner, D., Shinde, S., Asanovic, K., and Song, D. (2020, April 27-30). <i>Keystone: an open framework for architecting trusted execution environments</i> [Conference paper]. EuroSys '20: Fifteenth EuroSys Conference, Heraklion, Greece. https://doi.org/10.1145/3342195.3387532 .
LF2018	Kline, J., Balatsko, D., Mender, D., and Hoang, T. (2018). The Automotive Grade Linux software defined connected car architecture. The Linux Foundation. https://www.automotivelinux.org/wp-content/uploads/sites/4/2018/06/GoogleDrive_The-AGL-software-defined-connected-car-architecture.pdf .
Maene2017	Maene, P., Götzfried, J., de Clercq, R., Müller, T., Freiling, F., and Verbaauwhede, I. (2017). Hardware-based trusted computing architectures for isolation and attestation. <i>IEEE Transactions on Computers</i> , 67(3), 361-374. https://ieeexplore.ieee.org/document/7807249 .
NISTIR8320	NISTIR 8320, Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases
NISTSand	NIST Computer Security Resource Center Glossary, Sandbox definitions
NISTTCB	NIST Computer Security Resource Center Glossary, Trusted Computing Base definitions
NISTTrustA	NIST Computer Security Resource Center Glossary, Trust Anchor definitions
Perez2013	Perez-Botero, D., Szefer, J., and Lee, R.B. (2013). Characterizing hypervisor vulnerabilities in cloud computing servers. In <i>Cloud Computing '13: Proceedings of the 2013 international workshop on security in cloud computing</i> (pp. 3-10). https://doi.org/10.1145/2484402.2484406 .
Pinto2019	Pinto, S., and Santos, N. (2019). Demystifying Arm TrustZone: a comprehensive survey. <i>ACM Computing Surveys</i> , 51(6), 1-36. https://doi.org/10.1145/3291047 .
Pinto2020	Pinto, S., and Garlati, C. (2020). <i>Multi zone security for Arm Cortex-M devices</i> [Conference paper]. Embedded World Conference 2020, Nuremberg, Germany. https://www.researchgate.net/publication/339784921_Multi_Zone_Security_for_Arm_Cortex-M_Devices .
Sabt2015	Sabt, M., Achemlal, M., and Bouabdallah, A. (2015, August 20-22). <i>Trusted execution environment: what it is, and what it is not</i> [Conference paper]. 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland. https://doi.org/10.1109/Trustcom.2015.357 .
Sucio2020	Suciu, D., McLaughlin, S., Simon, L., and Sion, R. (2020). <i>Horizontal Privilege Escalation in Trusted Applications</i> [Conference paper]. 29th USENIX Security Symposium.
TCG	Trusted Computing Group (TCG), TCG Mobile Reference Architecture, version 2, revision 45.

TFA	TrustedFirmware, Trusted Firmware-A Documentation, https://trustedfirmware-a.readthedocs.io/en/latest/
TFM	TrustedFirmware, Trusted Firmware-M Documentation, https://trustedfirmware-m.readthedocs.io/en/latest/index.html
Tank2019	Tank, D., Aggarwal, A., and Chaubey, N. (2019). Virtualization vulnerabilities, security issues, and solutions: a critical study and comparison. <i>International Journal of Information Technology</i> , 14, 847-862. https://doi.org/10.1007/s41870-019-00294-x .
Yao2020	Yao, J., and Zimmer, V. (2020). <i>Building secure firmware: armouring the foundation of the platform</i> (1st ed). Apress. https://doi.org/10.1007/978-1-4842-6106-4 .

3. DEFINITIONS

The following provides further refinement of definitions of terms for the purpose of SAE J3101-2.

TRUSTED APPLICATION: A TA is one which has been authenticated and validated before being authorized to execute within the HPSE “protected environment” and is isolated from the “normal environment” as well as from other “TAs” within the “protected environment.”

SANDBOX: A system that allows an untrusted application to run in a highly controlled environment where the application's permissions are restricted to an essential set of computer permissions [NISTSand].

TRUSTED APPLICATION SECURE COMMUNICATIONS: An authenticated privileged communication mechanism between TAs.

TRUSTED APPLICATION DOMAIN ISOLATOR: The hardware enforced security boundary for a single TA or a group of mutually trusted TAs [GPD_SPE_009].

HPSE TRUST APPLICATION PROVISIONING MANAGER (HPM): A Trust Application provisioning manager (HPM) which is operated by the OEM.

HPSE AGENT (HA): A software component in the HPSE which manages the installation and updating of TAs.

HPSE BROKER (HB): A software component to relay or proxy trusted communication between the HPM and HA.

HPSE TRUST ANCHOR (HTA): An Authoritative entity which establishes a chain of trust between the HPM and HA [NISTTrustA].

TRUST DOMAIN (TD): The TA boundary and associated privileges for a single TA or a group of mutually trusted TAs.

4. SAE INFORMATION REPORTS MAPPING

The documents in Figure 1 provide information to support requirements within SAE J3101.

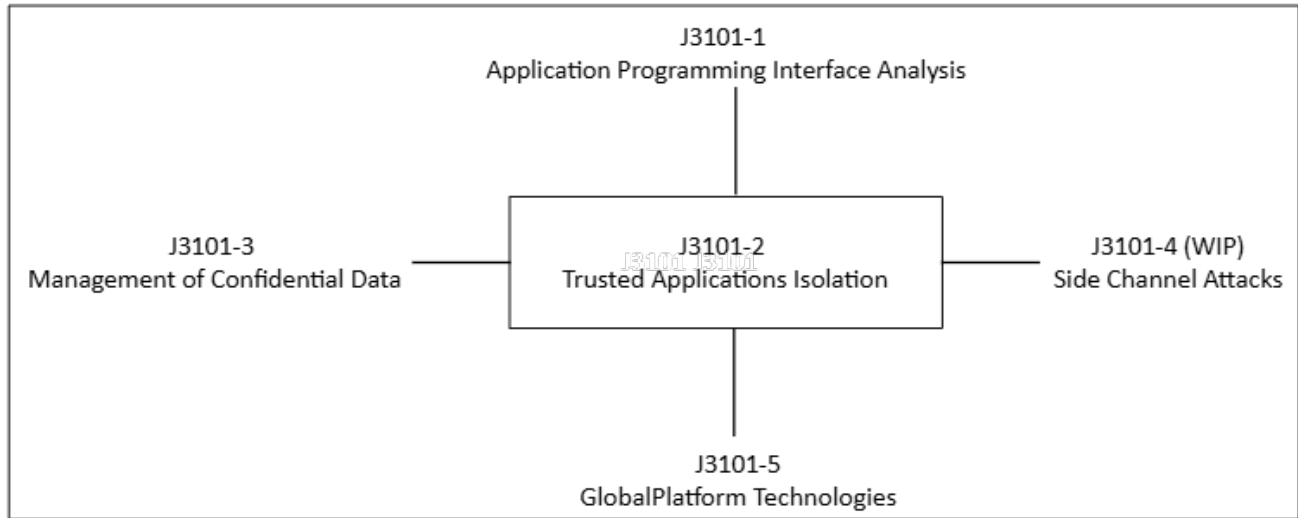


Figure 1 - SAE J3101 hardware protected security for ground vehicles information reports

4.1 Management of Confidential Data

The Hardware Protected Security Environment Management of Confidential Data information report SAE J3101-3 identifies a taxonomy and types of confidential data which must be protected. This data may be an asset of a TA or maybe an asset of the Secure Execution Environment. The TA and Secure Execution Environment assets must be protected from a confidentiality, integrity perspective and access to the assets authenticated. Identifying the assets and assessing the TA risk profile are critical to secure isolation of TAs and protection of the Secure Execution Environment. The Hardware Protected Security Environment Management of Confidential Data information report can be used to identify the assets to be protected when it is used, at rest, and in transit in the context of TA Isolation within a HPSE. An example of an HPSE asset is the keystore which must ensure strong isolation and access control to each TAs cryptographic keys and certificates.

4.2 Side Channel Attacks Resistance

The Side Channel Attacks Resistance information report SAE J3101-4, which is a work in progress (WIP), provides a survey and taxonomy of side channel and fault injection attacks which impact the automotive industry. It also provides a taxonomy of countermeasures and guidance on appropriate mitigation techniques to be considered by manufacturers.

4.3 Application Programming Interface Analysis

The Application Programming Interface Analysis information report SAE J3101-1 gives an understanding of the software Application Programming Interface (API) landscape for SAE J3101 devices in relation to automotive-relevant crypto APIs. This report can be used to understand the APIs relevant to TAs access external and internal to the HPSE.

4.4 Global Platform Technologies

The Global Platform Technologies information report SAE J3101-5 provides a coverage of existing Global Platform Secure Element (SE) and Trusted Execution Environment (TEE) technologies APIs for implementing requirements within SAE J3101.