



SURFACE VEHICLE INFORMATION REPORT

J3101™-3

JUL2024

Issued

2024-07

Hardware Protected Security Environment Management of Confidential Data

RATIONALE

A vehicle component could contain and use several types of confidential data: secret elements such as customer identification, keys, and any confidential data for applications. These data elements could be stored in the hardware protected security environment (HPSE) or outside of HPSE. While SAE J3101 provides guidance and requirements on key management inside HPSE, providing more technical guidance on the management of information identified as confidential data could help stakeholders. The definition of confidentiality is in Section 3. Additionally, confidential data management could be based on OEM policy and government regulations. The scope of this information report is to address the current state of the art in managing confidential data in technical and regulatory aspects. The report will identify and discuss as enumerated below.

- Common principles of data confidentiality are outlined in one or more informative illustrative examples to provide the context of the role of an HPSE.
- SAE J3101 hardware support for technical aspects of secure management of confidential data.
- SAE J3101 hardware support necessary for secure deletion/erase.
- SAE J3101 hardware to achieve consistent secure management of confidential data.
- Achieve conformance with common principles in privacy regulations and standards.
- Describe use cases for confidential data management.

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 J3101-3_202407

For more information on this standard, visit
https://www.sae.org/standards/content/J3101-3_202407

Documents

Standard, visit Sharing Hub

TABLE OF CONTENTS

1.	SCOPE.....	4
2.	REFERENCES.....	4
2.1	Applicable Documents	4
2.1.1	SAE Publications.....	4
2.2	Other Publications.....	4
3.	DEFINITIONS	6
4.	CONFIDENTIAL DATA MANAGEMENT OVERVIEW.....	8
4.1	Confidential Data.....	8
4.2	Methodologies to Manage Confidential Data.....	11
5.	HPSE CONFIDENTIAL DATA MANAGEMENT	11
5.1	Environment in HPSE	11
5.1.1	Process	12
5.1.2	Storage.....	12
5.2	Confidential Data Management in Each Data State	12
5.2.1	Confidential Data at Rest	13
5.2.2	Confidential Data in Use	13
5.2.3	Confidential Data in Transit (Informative)	13
6.	COMMON PRINCIPLES OF HPSE CONFIDENTIAL DATA MANAGEMENT	13
6.1	Methodologies to Manage Confidential Data.....	13
6.1.1	Encryption	14
6.1.2	Homomorphic Encryption.....	15
6.1.3	Pseudonymization.....	15
6.1.4	Anonymization.....	16
6.1.5	Suppression	17
6.1.6	Generalization	17
6.1.7	K-Anonymity.....	18
6.1.8	Access Control	18
6.1.9	Zeroization/Sanitization.....	19
6.2	Scenarios in Managing Confidential Data.....	20
6.2.1	Confidential Data Management within HPSE	20
6.2.2	Confidential Data Management Between Two Trusted Applications in the Same HPSE	20
6.2.3	Confidential Data Management Between Two HPSEs.....	21
6.2.4	Data Management Between HPSE and Normal Environment	22
7.	CONFIDENTIAL DATA MANAGEMENT IN SAE J3101	22
8.	CONFORMANCE OF CONFIDENTIAL DATA MANAGEMENT	23
8.1	Common Principles in Privacy Regulations	23
8.1.1	General Data Protection Regulation (GDPR)	23
8.1.2	UNECE WP29: OTP Protection Profile of an Automotive Gateway	24
8.2	Comparison with the Common Principles in Other Standards	24
8.2.1	Network Functions Virtualization (NFV) Security by ETSI ISG.....	24
8.2.2	Trusted Platform Module by Trusted Computing Group	26
9.	USE CASES FOR CONFIDENTIAL DATA MANAGEMENT.....	27
9.1	Implementation of HPSE.....	27
9.2	Use Cases of Confidential Data Management.....	27
9.2.1	Keyless Entry ECU.....	27
9.2.2	Secure Storage	28
9.2.3	Secure Erase	28
9.2.4	IP Protection.....	28
9.2.5	Secure Logging	28

9.2.6	PII Management.....	28
9.2.7	Encrypted Boot.....	29
9.2.8	Key Management.....	30
10.	NOTES.....	31
10.1	Revision Indicator.....	31
APPENDIX A	CRYPTOGRAPHIC KEY PROTECTION.....	32
APPENDIX B	ALGORITHMS AND PROTOCOLS.....	37
APPENDIX C	RANDOM NUMBER GENERATION.....	38
APPENDIX D	NONVOLATILE CRITICAL SECURITY PARAMETERS.....	39
APPENDIX E	CRYPTOGRAPHIC ALGORITHM AGILITY.....	40
APPENDIX F	INTERFACE CONTROL.....	41
APPENDIX G	SECURE EXECUTION ENVIRONMENT.....	42
APPENDIX H	SELF-TEST.....	44
Figure 1	Data states: Data in Use, Data at Rest, and Data in Transit.....	12
Figure 2	Encryption.....	14
Figure 3	Homomorphic encryption.....	15
Figure 4	Pseudonymization.....	16
Figure 5	Anonymization.....	16
Figure 6	Suppression.....	17
Figure 7	Generalization.....	17
Figure 8	K-anonymity.....	18
Figure 9	Access control.....	19
Figure 10	Confidential data management scenarios.....	20
Figure 11	Multiple trust applications (processes) in the same HPSE.....	21
Figure 12	Confidential data management between two HPSE.....	21
Figure 13	Data management between HPSE and normal environment.....	22
Figure 14	Types of HPSE implementations in SoCs.....	27
Figure 15	Flow of PII management in SAE J3101.....	29
Figure 16	Flows encrypted boot associated with HPSE.....	30
Table 1	Examples of confidential data.....	8
Table 2	Taxonomy and types of confidential data.....	9
Table 3	Methodologies to manage confidential data.....	11
Table 4	Data in encryption.....	14
Table 5	Data in homomorphic encryption.....	15
Table 6	Data in pseudonymization.....	16
Table 7	Data in anonymization.....	17
Table 8	Data in suppression.....	17
Table 9	Data in generalization.....	18
Table 10	Data in k-anonymity.....	18
Table 11	Data in access control.....	19
Table 12	SAE J3101 requirements related to confidential data management.....	23
Table 13	Topics addressed in SAE J3101 related to confidential data management.....	30

1. SCOPE

This document provides an information report to the readers for the management of confidential data associated with hardware protected security environment (HPSE). The scope of the present document is common principles of confidential data, methodologies, conformance of SAE J3101 with regulations and standards, and use cases.

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

ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering

2.2 Other Publications

44 U.S.C., Sec. 3542 Title 44 United States Code, Section 3542 - Definitions

CCCDKR3 Car Connectivity Consortium Digital Key Release 3 - Technical Specification Version 1.1.0

CNSSI 4009-2015 Committee on National Security Systems (CNSS) Glossary

ETSI_NFV-SEC009 ETSI GS NFV-SEC 009 V1.1.1 (Network Functions Virtualization (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration.

FIA_PP_AG2020 Federation Internationale De L'automobile OTP Protection Profile of an Automotive Gateway v1.02, WP. 29-181-10 181st WP.29, June 2020.

FIPS140-2 Security Requirements for Cryptographic Modules (March 2001)

FIPS140-3 Security Requirements for Cryptographic Modules (March 2019)

FIPS186-5 Digital Signature Standard (DSS)

FIPS201-3 Personal Identity Verification (PIV) of Federal Employees and Contractors

GDPR General Data Protection Regulation, <https://gdpr-info.eu/>.

GPD_SPE_009 GlobalPlatform TEE System Architecture v1.3 - GPD_SPE_009 (May 2002)

GUARDIAN2018 Hern, Alex (2018, January 28). Fitness tracking app Strava gives away location of secret U.S. army bases. *The Guardian*.

HESTANDARD Homomorphic Encryption Standardization

IDSC International Data Sanitization Consortium, Data Sanitization Terminology and Definitions

ISO/IEC19790-2012 ISO/IEC 19790:2012, Information technology - Security techniques - Security requirements for cryptographic modules - Technical Corrigendum 1

ISO/IEC27000:2016	ISO/IEC 27000:2016, Information technology - Security techniques - Information security management systems - Overview and vocabulary
ISO/TS 25237:2008	ISO/TS 25237:2008, Health informatics - Pseudonymization
NISTIR7316	NISTIR 7316, Assessment of Access Control Systems
NISTIR7695	NISTIR 7695, Common Platform Enumeration: Naming Specification Version 2.3
NISTIR8053	NISTIR 8053, De-Identification of Personal Information
NISTSP800-56BR2	NIST SP 800-56B Rev. 2, Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography
NISTSP800-57P1	NIST SP 800-57 Part 1 Rev. 5, Recommendation for Key Management: Part 1 - General
NISTSP800-57P2R1	NISTSP 800-57 Part 2 Rev. 1, Recommendation for Key Management: Part 2 - Best Practices for Key Management Organizations
NISTSP800-122	NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
NISTSP800-128	NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
NISTSP800-133R2	NIST SP 800-133 Rev. 2, Recommendation for Cryptographic Key Generation
NISTSP800-150	NIST SP 800-150, Guide to Cyber Threat Information Sharing
NISTSP800-160	NIST SP 800-160 Vol. 1 Rev. 1, Engineering Trustworthy Secure Systems
NISTSP800-175B	NIST SP 800-175B Rev. 1, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms
NISTSP800-192	NIST SP 800-192, Verification and Test Methods for Access Control Policies/Models
NISTSP1800-10B	NIST SP 1800-10, Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector
RFC 4949	Internet Security Glossary, Version 2
SW2019	Williams, E.A. (2019, April 26). Data in Use Is the Point of Least Resistance. <i>Security Week</i> . https://www.securityweek.com/data-use-point-least-resistance
TPM_2.0_2019	TPM 2.0 1.59 revision, November 2019.
Boneh2013	Boneh, D., Gentry, C., Halevi, S., Wang, F., Wu, D.J. (2013). Private Database Queries Using Somewhat Homomorphic Encryption. <i>Lecture Notes in Computer Science</i> , 7954. Springer. https://doi.org/10.1007/978-3-642-38980-1_7
Chen2017	Chen, S., Zhang, X., Reiter, M., and Zhang, Y. (2017). <i>Detecting Privileged Side-Channel Attacks in Shielded Execution with Déjà Vu</i> [Conference paper]. 2017 ACM on Asia Conference on Computer and Communications Security (ASIA CCS '17), New York, NY, USA.
Chow02AES	Chow, S., Eisen, P.A., Johnson, H., and van Oorschot, P.C. (2002). White-Box Cryptography and an AES Implementation. In Proceedings of the 9th International Workshop on Selected Areas in Cryptography (SAC 2002). <i>Lecture Notes in Computer Science</i> , 2595, 250-270, Springer.

- Chow02DES Chow, S., Eisen, P.A., Johnson, H., and van Oorschot, P.C. (2002). A white-box DES implementation for DRM applications. In Proceedings of the ACM Workshop on Security and Privacy in Digital Rights Management (DRM 2002). *Lecture Notes in Computer Science*, 2696, 1-15, Springer.
- Gentry2009 Gentry, C. (2009). *Fully homomorphic encryption using ideal lattices* [Conference paper]. 41st annual ACM symposium on Theory of computing (STOC '09), New York, NY, USA. <https://doi.org/10.1145/1536414.1536440>
- Sweeney2022-1 Sweeney, L. (2022). Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5), 571-588.
- Sweeney2022-2 Latanya Sweeney, L. (2002). k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5), 557-570.
- Tibouchi2014 Tibouchi, M. (2014). *Fully Homomorphic Encryption over the Integers: From Theory to Practice*. NTT Technical Review.
- Zaheri2022 Zaheri, M., et al (2022). *Targeted Deanonymization via the Cache Side Channel: Attacks and Defenses* [Conference paper]. 31st USENIX Security Symposium (USENIX Security 22).

3. DEFINITIONS

ACCESS CONTROL: Procedures and controls that limit or detect access to critical information resources. This can be accomplished through software, biometrics devices, or physical access to a controlled space. [NISTSP800-192 under Access Control, NISTIR7316 under Access Control]

ANONYMIZATION: Process that removes the association between the identifying dataset and the data subject. [NISTIR8053, ISO/TS 25237:2008]

CERTIFICATE: A set of data that uniquely identifies a public key (which has a corresponding private key) and an owner that is authorized to use the key pair. The certificate contains the owner's public key and possibly other information and is digitally signed by a Certification Authority (i.e., a trusted party), thereby binding the public key to the owner. [FIPS186-5 under Certificate]

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]

A property of information that is not made available or disclosed to unauthorized individuals, entities, or processes. [ISO/IEC27000:2016]

The property that sensitive information is not disclosed to unauthorized entities (i.e., the secrecy of key information is maintained). [NISTSP800-175B Rev. 1 under Confidentiality]

CONFIGURATION: The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged. [NISTSP800-128]

CONFIGURATION ITEM: An item or aggregation of hardware or software or both that is designed to be managed as a single entity. Configuration items may vary widely in complexity, size, and type, ranging from an entire system - including all hardware, software, and documentation - to a single module, a minor hardware component, or a single software package. [NISTIR7695 under Configuration Item from ISO/IEC19770-2 - adapted]

CRITICAL SECURITY PARAMETER (CSP): Security-related information whose disclosure or modification can compromise the security of a cryptographic module. [ISO/IEC 19790:2012]

Security-related information whose disclosure or modification can compromise the security of a cryptographic module. Domain parameters, secret or private keys, shared secrets, key-derivation keys, intermediate values, and secret salts are examples of quantities that may be considered critical security parameters in this recommendation. [NISTSP800-56BR2 under Critical security parameter (CSP)]

ENCRYPTION: Cryptographic transformation of data (called “plaintext”) into a form (called “ciphertext”) that conceals the data’s original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called “decryption,” which is a transformation that restores encrypted data to its original state. [NISTSP800-82 Rev. 2 under Encryption, RFC 4949]

EPHEMERAL KEY: A cryptographic key that is generated for each execution of a key-establishment process and that meets other requirements of the key type (e.g., unique to each message or session). [NISTSP800-57P2R1]

FIRMWARE: Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs. [NISTSP1800-10B under Firmware from CNSSI 4009-2015]

GENERALIZATION: Aggregating multiple records into the broader category.

HOMOMORPHIC ENCRYPTION: A form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext. [Tibouchi2014]

INTELLECTUAL PROPERTY: Creations of the mind such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under intellectual property law, the holder of one of these abstract “properties” has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered. [CNSSI 4009-2015]

K-ANONYMITY: Each released record in a set of K records has at least (k-1) other records in the release whose values are indistinct over those fields that appear in external data.

PERSONALLY IDENTIFIABLE INFORMATION (PII): Information that can be used to distinguish or trace an individual’s identity - such as name, social security number, biometric data records - either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (e.g., date and place of birth, mother’s maiden name, etc.). [FIPS201-3 under Personally Identifiable Information (PII) from OMB M-17-12 - adapted]

PRIVATE KEY: The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. [FIPS201-3 under Private Key]

PROCESS: Set of interrelated or interacting activities that use inputs to deliver an intended result. [NISTSP800-160 from ISO 9000:2015]

PSEUDONYMIZATION: A particular type of deidentification that both removes the association with a data subject and adds an association between a particular set of characteristics relating to the data subject and one or more pseudonyms. [NISTIR8053, ISO/TS 25237:2008 adapted]

PUBLIC KEY: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. [FIPS201-3 under Public Key]

PUBLIC SECURITY PARAMETER (PSP): Security-related public information whose modification can compromise the security of a cryptographic module. [ISO/IEC 19790:2012]

SENSITIVE INFORMATION: Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act) but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [NISTSP800-150 under Sensitive Information]

SENSITIVE SECURITY PARAMETERS (SSP): SSP includes Critical Security Parameters (CSP) and Public Security Parameters (PSP). [ISO/IEC19790-2012]

STORAGE: Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered and from which data may be retrieved. [NISTSP800-88 Rev. 1]

SUPPRESSION: The process of systematically removing a field or replacing it with a value in a way that does not preserve the analytic utility of the value, such as replacing a phone number with asterisks or a randomly generated pseudonym. [NISTIR8053]

SYMMETRIC KEY: A cryptographic key used by one or more (authorized) entities in a symmetric-key cryptographic algorithm; the key is not made public. [NISTSP800-133R2]

ZEROIZATION/SANITIZATION: A method of erasing electronically stored data, cryptographic keys, and critical security parameters by altering or deleting the contents of the data storage to prevent recovery of the data. [FIPS140-3]

4. CONFIDENTIAL DATA MANAGEMENT OVERVIEW

SAE J3101 addresses confidentiality as the required property for keys and describes encryption as the method to keep the keys secret and preserve their confidentiality and as the method of confidential data management. It also defines that the simplest HPSE must have the capability to encrypt data within the protected environment and keep the key used to perform the encryption similarly protected.

While encryption and access control are addressed to manage confidential data in SAE J3101, there are more types of data to be considered as confidential data and also more methodologies to manage those confidential data to preserve their confidentiality.

This section discusses the categories of confidential data and the methodologies to manage them.

4.1 Confidential Data

Confidential data is defined as any information that is not intended for public dissemination and information that needs to preserve its confidentiality.

By the definition of “confidentiality,” examples of confidential data may include (see Table 1):

Table 1 - Examples of confidential data

Data that requires confidentiality	Category
Personally Identifiable Information (PII) (Protecting Personal Privacy under [44 U.S.C., Sec. 3542])	PII
Proprietary information (under [44 U.S.C., Sec. 3542])	Data
Information that is not made available or disclosed to unauthorized individuals, entities, or processes (under [ISO/IEC27000:2016])	Data
Sensitive information (under [NIST SP 800-175B])	PII
Key information (under [NIST SP 800-175B])	Key

Upon the definitions of confidentiality from the various sources, this report categorizes the confidential data in Table 2.

Key is separated into Crypto Key and Parameter. Crypto Key is the group of keys, while Parameter is the group of terms used in [ISO/IEC19790]. Data is separated into Data and Messaging.

Table 2 - Taxonomy and types of confidential data

Taxonomy	Type	Considered as Confidential data	Note
Crypto Key	Symmetric key	Y	Addressed in SAE J3101
	Public key and certificate	N	Addressed in SAE J3101
	Private key	Y	Addressed in SAE J3101
	Ephemeral Key	Y	Addressed in SAE J3101 Note that any private keys or symmetric keys used for a limited period could be considered ephemeral.
Parameter	Sensitive Security Parameters (SSP)	CSP only	SSPs consist of CSPs and PSPs, appears in [ISO/IEC19790-2012].
	Critical Security Parameters (CSP)	Y	Addressed in SAE J3101 as Nonvolatile Critical Security Parameters
	Public Security Parameters (PSP)	N	PSPs do not require protection from unauthorized access, use, and disclosure. [ISO/IEC19790-2012] Example: Public cryptographic keys, public key certificates, self-signed certificates, trust anchors, one-time passwords associated with a counter, and internally held date and time.
PII	Personally Identifiable Information (PII)	Y	Any representation of information that could identify an individual directly or indirectly could be considered as PII. Manage it separately. Example: Driver's information, biometric information.
	Sensitive Information/Data	Y	Sensitive information such as controlled unclassified information (CUI) and personally identifiable information (PII) may be encountered when handling cyber-threat information. The improper disclosure of such information could cause financial loss; violate laws, regulations, and contracts; be cause for legal action; or damage an organization or individual's reputation. [NISTSP800-150]
	Location data	Depends on the use cases	If the location of the vehicle is exposed, it could impact the user's privacy. [GUARDIAN2018] Could be related to PII, but it is managed separately in this report. Location data of individual and device can be distinct.
Data	Configuration data	Depends on the specific data	Implementation specific. Depending on the application, configuration data could be sensitive, such as calibration files/data, whose unauthorized modification could cause

			safety, financial, operational, and privacy (S, F, O, P) damage. [ISO/SAE21434] Example: Calibration data could be confidential. Provisioning virtual machines or containers could be confidential [ETSI_NFV-SEC009]. [FIA_PP_AG2020] addresses the threat that attacker disclosure configuration data to achieve the modification.
	Firmware	Implementation specific	Firmware could be any executable code run by a microcontroller and be inclusive of basic software, middleware, applications, or scripts. Firmware in NVM (Nonvolatile Memory) or persistent storage can be updated by an executing program but survives in power cycling. Firmware may need confidentiality depending on the use cases: • IP could be associated with source code of the firmware. • Encrypted boot stores the firmware in encrypted state in data at rest (e.g., full disk encryption, encrypted boot partition) • Encrypted binary is used during OTA update. Example: [FIA_PP_AG2020] addresses the threat that attacker disclosure firmware to achieve the modification.
	Intellectual Property	Depends on the use cases	The intellectual property (IP) protection use case aims to prevent an adversary gaining access to the plain text firmware or software. [SAE J3101] Note that cloning does not violate confidentiality, but it constitutes a violation of intellectual property rights as it involves making unauthorized copies. To prevent cloning, digital rights management (DRM) technologies can be used, such as licensing keys that cannot be easily cloned. It's important to be aware of these issues and to take appropriate measures to protect intellectual property.
Messaging	In-vehicle Message	Some; depends upon how it is implemented	SAE J3101 addresses that in-vehicle message optionally requires confidentiality so that the message content can only be read by the legitimate destination node(s). [FIA_PP_AG2020] addresses the threat that attacker disclosure in-vehicle message to violate privacy.
	External Message	Depends on the use cases	Data coming from the outside of the vehicle. Examples: Traffic messages, software update command, service data, etc.

4.2 Methodologies to Manage Confidential Data

Encryption and access control are addressed in SAE J3101 as methodologies to manage information identified as confidential data.

SAE J3101 addresses the following mandatory common requirements for the encryption of confidential data:

- Key protection
- Cryptographic algorithms: symmetric key algorithms
- Secure execution environment
- Appropriate self-tests

However, certain types of confidential data, such as PII, may require more methodologies to preserve confidentiality and privacy. Thus, this report investigates more methodologies to manage confidential data (see Table 3).

Table 3 - Methodologies to manage confidential data

Methodology		Applicable to manage...	Refer to...	Addressed in SAE J3101
Encryption	Encryption	Crypto Keys, Parameters, PII, Data, Messaging	Section 6.1.1	Y
	Homomorphic encryption	PII, Data, Messaging	Section 6.1.2	N
Deidentification	Pseudonymization	PII	Section 6.1.3	N
	Anonymization		Section 6.1.4	N
	Suppression		Section 6.1.5	N
	Generalization		Section 6.1.6	N
	K-anonymity		Section 6.1.7	N
Access control		Crypto Keys, Parameters, PII, Data, Messaging	Section 6.1.8	Y
Zeroization/Sanitization		Crypto Keys, Parameters, PII, Data, Messaging	Section 6.1.9	Y
Key Management		Crypto Keys, Parameters	SAE J3101	Y

5. HPSE CONFIDENTIAL DATA MANAGEMENT

HPSE confidential data management preserves the confidentiality of data associated with HPSE at each data state (i.e., Data in Use, Data at Rest, and Data in Transit).

5.1 Environment in HPSE

SAE J3101 defines that HPSE offers at least one mechanism of security, implemented by hardware support, and may be leveraged or extended further by firmware. HPSE includes RAM, key storage, etc. This report simplifies the model into process and storage.

5.1.1 Process

Process is defined as a set of interrelated or interacting activities that use inputs to deliver an intended result. A process or processes in HPSE is in the scope of this report.

Examples of processes are:

- Security mechanism(s) (i.e., key generation, encryption/decryption, signing/verifying, unsealing - decryption to the correct boot state, sealing - encryption, attestation, etc.)
- Methodologies in Table 3
- Protected capability [TPM_2.0_2019]

5.1.2 Storage

Storage is defined as a retrievable retention of data. This report uses storage as the state that data is stored in persistent state in HPSE.

Examples of storage are:

- Key storage (in HPSE)
- Storage in HPSE or shielded location in HPSE [TPM_2.0_2019]
- NVM

NOTE 1: It is reported that side-channel attacks could happen at a shielded location. [Chen2017]

NOTE 2: Storing data in a normal environment in an encrypted state could be considered storage. [TPM_2.0_2019] specifies this case as a protected location.

NOTE 3: Data is stored in non-persistent state such as RAM, CPU caches, or CPU registers as Data in Use state.

5.2 Confidential Data Management in Each Data State

Confidential data management can be distinguished by the data state as Data in Use, Data at Rest, and Data in Transit, as illustrated in Figure 1.

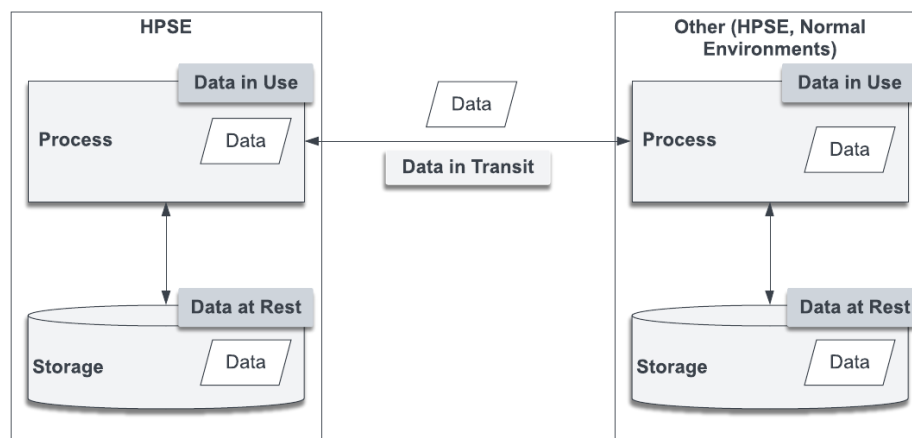


Figure 1 - Data states: Data in Use, Data at Rest, and Data in Transit



Documents

Document Sharing Hub

5.2.1 Confidential Data at Rest

This report considers Data at Rest as the confidential data in Storage and not in use by Process inside of HPSE.

SAE J3101 mentions the requirement for protection of Data at Rest state for the Secure Storage.

- The data should be encrypted at rest with a key that is securely stored, as discussed in 6.2
- There should be a separate and distinct key for each owning entity.
- Data may be integrity protected at rest.

SAE J3101 also describes use cases storing PII, IP, and firmware in an encrypted state.

5.2.2 Confidential Data in Use

Data in Use could be the most vulnerable point to various attacks [SW2019]. This report considers Data in Use as confidential data being processed by Process inside of HPSE.

SAE J3101 addresses the management of key materials in use.

For PII, SAE J3101 addresses the use case of “access to personally identifiable information” and shows the management of PII using encryption/decryption.

For the firmware, SAE J3101 addresses the use case of “Intellectual Property Protection” to prevent the disclosure of the plaintext software or firmware to the adversary, using the encryption and access control.

5.2.3 Confidential Data in Transit (Informative)

The Data in Transit through communication mediums from the source (OEM/Service Provider) to the destination (ECU) is beyond the scope of SAE J3101.

However, how HPSE facilitates the confidential data transmission to other entities and confidential data between HPSE and other external entities, such as other HPSE or normal environment applications, may need to be considered as the data management “before in transit” state.

6. COMMON PRINCIPLES OF HPSE CONFIDENTIAL DATA MANAGEMENT

Common principles of confidential data management could be using appropriate methodology considering the scenarios.

6.1 Methodologies to Manage Confidential Data

The following methodologies can be considered for Confidential Data Management:

- Encryption
- Homomorphic encryption
- Pseudonymization
- Anonymization
- Masking suppression
- Generalization
- K-anonymity

- Access control
- Zeroization/sanitization
- Key management

NOTE: Key management is omitted as SAE J3101 has comprehensive requirements.

6.1.1 Encryption

Encryption is a common process to manage the confidential data.

Plaintext could be generated inside or outside of HPSE. For confidential data, plaintext needs to be stored in storage inside of HPSE.

For keys, either symmetric keys or asymmetric keys (public key, private key) are used.

When the symmetric key is used, the encryption process must be done in HPSE.

If the encryption of confidential data is done using the public key, encryption still needs to be done inside of HPSE.

The ciphertext can be stored outside of HPSE.

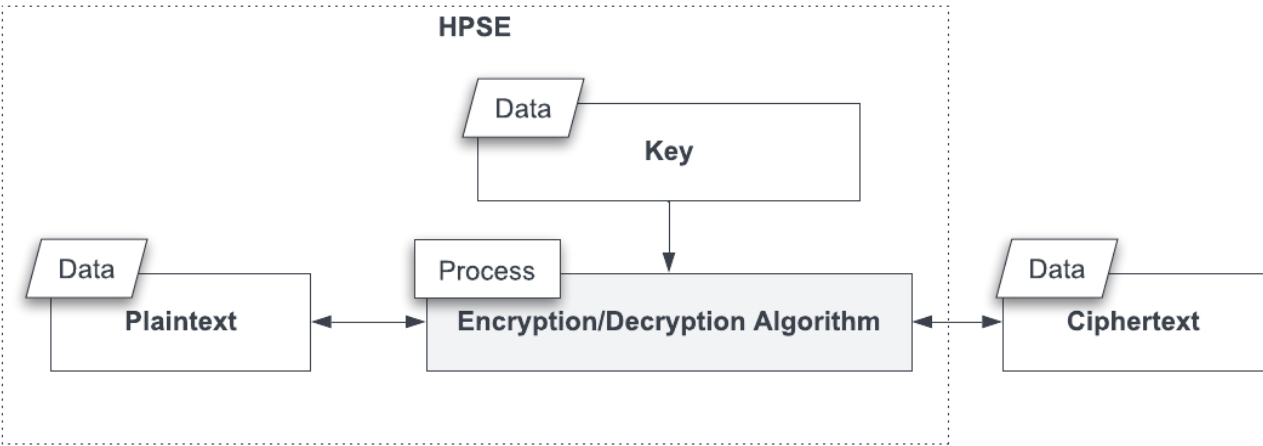


Figure 2 - Encryption

Table 4 - Data in encryption

	HPSE	Normal Environment
Data at rest	Symmetric key Public key (Encryption) Private key (Decryption) Plaintext	Ciphertext (Output)
Data in use	Symmetric key Public key (Encryption) Private key (Decryption) Plaintext (Encryption) Ciphertext (Decryption)	Ciphertext (Input)