



SURFACE VEHICLE INFORMATION REPORT

J3101™-5

SEP2025

Issued

2025-09

Hardware Protected Security Environment -
GlobalPlatform Technologies 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 GlobalPlatform technologies – Secure Elements (SE) and Trusted Execution Environment (TEE).

EXECUTIVE SUMMARY

SAE's TEVEES18B Vehicle Electrical Hardware Security Task Force has conducted a review of how GlobalPlatform Secure Elements (SEs) and Trusted Execution Environments (TEEs) specifications align with SAE J3101 requirements for Hardware Protected Security Environments for Ground Vehicles.

This analysis demonstrates a strong alignment between GlobalPlatform technologies and SAE J3101 requirements with a direct correspondence of:

- 81% of the Overall Requirements Satisfied by Certified Secure Element Products
- 76% of the Overall Requirements Satisfied by Certified Trusted Execution Environment Products

Moreover, a GlobalPlatform compliant platform also provides the tools for the development of secure trusted applications which directly satisfy an additional increment of the SAE J3101 requirements:

- An additional 19% (100% in total) are satisfied by Certified Secure Element Products coupled with a suitable trusted application.
- An additional 22% (98% in total) are satisfied by Certified Trusted Execution Environment Products coupled with a suitable trusted application.

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: 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 J3101-5_202509

For more information on this standard, visit https://www.sae.org/standards/content/J3101-5_202509/

Documents

Standard, visit Sharing Hub

Finally, within the remaining 2% and 5%, respectively, is self-test; GlobalPlatform has indicated that there are at least two possible ways to use the platform and tools to ensure solutions are in a known good state and that this can be achieved by:

- Cryptographic validation that the code is unmodified from a known good state prior to use of the system (the ISO 15408 Common Criteria Approach); or
- A combination of cryptographic validation of a known good set of tests/expected results and evaluation of those tests prior to use of the system (the FIPS approach).

See Appendix B for further explanation of these requirements.¹

TABLE OF CONTENTS

1.	SCOPE.....	3
2.	REFERENCES.....	3
2.1	Applicable Documents	3
2.1.1	SAE Publications.....	3
2.1.2	BSI Publications	3
2.1.3	IEEE Publications.....	3
2.1.4	IETF Publications	3
2.1.5	ISO/IEC Publications.....	3
2.1.6	NIST Publications.....	4
2.1.7	GlobalPlatform Publications.....	4
3.	METHODOLOGY	4
3.1	Requirements Categorization	4
3.2	Interpreting Coverage Analysis	5
3.2.1	Interpreting Non-Covered Requirements.....	6
4.	MAPPING OF GLOBALPLATFORM TECHNOLOGY SUPPORT WITH COMMENTS	7
5.	NOTES	25
5.1	Revision Indicator.....	25
APPENDIX A	ADDITIONAL BACKGROUND CHARACTERISTICS FOR GLOBALPLATFORM TECHNOLOGIES.....	26
APPENDIX B	AN AREA FOR DISCUSSION: SELF-TEST VERSUS COMMON CRITERIA.....	28
Figure 1	Percentage of fulfilment of SAE J3101 requirements by GlobalPlatform technologies (mandatory and optional requirements).....	6
Table 1	Coverage analysis categories.....	5

¹ These SAE J3101 requirements (11 in all) are satisfied by the development of secure Trusted Applications



1. SCOPE

The scope of the analysis is on the GlobalPlatform Secure Element (SE) and Trusted Execution Environment (TEE) standard specifications correspondence to SAE J3101 recommended practices. This analysis includes focuses on the platform specifications but not the scope of any future security application/applets. Both of these GlobalPlatform specifications have associated protection profiles to validate compliance, although GlobalPlatform does not currently have any specific SAE J3101 protection profiles. GlobalPlatform has communicated that it is assessing whether or not to develop application-level protection profiles to more explicitly cover the remaining requirements of SAE J3101 in order to allow for standardized testing and certification of complete solutions.

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 (U.S. and Canada only) or +1 724-776-4970 (Outside U.S. and Canada), www.sae.org.

SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems

SAE J3101 Hardware Protected Security for Ground Vehicles

2.1.2 BSI Publications

Available from BSI, PO Box 200363, 53133 Bonn, Germany, Tel: +49 228 9582-0, www.bsi.bund.de.

BSI-CC-PP-0084-2014 Security IC Platform Protection Profile with Augmentation Packages, Version 1.0

2.1.3 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

IEEE 1609.2 IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Application and Management Messages

2.1.4 IETF Publications

Copies of these documents are available online at www.rfc-editor.org.

RFC 8391 XMSS: eXtended Merkle Signature Scheme

2.1.5 ISO/IEC 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 IEC Secretariat, 3 rue de Varembe, PO Box 131, CH-1211 Geneva 20, Switzerland, Tel: +41 22 919 0211, www.iec.ch.

ISO/IEC 19790 Information security, cybersecurity and privacy protection - Security requirements for cryptographic modules

2.1.6 NIST Publications

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

FIPS 140-2 Security Requirements for Cryptographic Modules

2.1.7 GlobalPlatform Publications

Copies of these documents are available online at <https://globalplatform.org/specs-library/>.

GP TECHNOLOGY	DOCUMENT REFERENCE	TITLE	VERSION	REFERENCE LINK
SE	GPC_SPE_034	Card Specification [GPCS]	2.3.1	https://globalplatform.org/specs-library/card-specification-v2-3-1/
	GPC_SPE_174	Secure Element Protection Profile [SE PP]	1.0	https://globalplatform.org/specs-library/secure-element-protection-profile/
		GlobalPlatform Card API	1.7.1	https://globalplatform.org/specs-library/globalplatform-card-api-org-globalplatform/
TEE	GPD_SPE_009	TEE System Architecture [TEE Sys Arch]	1.3	https://globalplatform.org/specs-library/tee-system-architecture/
	GPD_SPE_010	GPD TEE Internal Core API [TEE Core]	1.3.1/1.4	https://globalplatform.org/specs-library/tee-internal-core-api-specification/
	GPD_SPE_021	TEE Protection Profile [TEE PP]	1.3	https://globalplatform.org/specs-library/tee-protection-profile-v1-3/
	GPD_SPE_025	TEE TA Debug Specification [TEE Debug]	1.0.1	https://globalplatform.org/specs-library/tee-ta-debug-specification-v1-0-1/
	GPD_SPE_120	TEE Management Framework (TMF) including ASN.1 Profile [TMF]	1.1.2	https://globalplatform.org/specs-library/tee-management-framework-including-asn1-profile-1-1-2/
	GPD_GUI_069	TEE Initial Configuration [TEE Config]	1.1	https://globalplatform.org/specs-library/tee-initial-configuration-v1-1/
	GPD_GUI_089	TMF Initial Configuration [TMF Config]	1.0	https://globalplatform.org/specs-library/tmf-initial-configuration-v1-0/
SE and TEE	GP_TEN_053	Cryptographic Algorithm Recommendations [Crypto Rec]	2.0	https://globalplatform.org/specs-library/globalplatform-technology-cryptographic-algorithm-recommendations/
	GP_REQ_025	Root of Trust Definitions and Requirements [RoT]	1.1.1	https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/

3. METHODOLOGY

3.1 Requirements Categorization

Each SAE J3101 requirement was separately categorized for GlobalPlatform Secure Elements and for Trusted Execution Environments. GlobalPlatform technology has different security layers, with some security services supported by the platform and others by Trusted Applications which run on the platform. For this reason, the fulfillment of requirements has been divided into three levels, evidencing the coverage (or not) of the different security layers.

Table 1 - Coverage analysis categories

SAE J3101 Requirement Fulfillment Level	Description of GlobalPlatform Categorization for the Mapping
Yes	This SAE J3101 requirement is fully covered by GlobalPlatform's compliant platform for Secure Elements or Trusted Execution Environments as indicated. These requirements are also supported by existing Common Criteria (CC) protection profiles.
Yes (TA)	Full alignment can be achieved through development of Trusted Applet/Application (TA) running on a GlobalPlatform compliant platform. Development of TA is an Innate Characteristic Supported by GlobalPlatform. GlobalPlatform is assessing whether to develop application-level protection profiles for these applications in order to more explicitly correspond to these requirements of SAE J3101, fostering standardized testing and certification of complete solutions.
No/Partially	These three SAE J3101 requirements are not fully met by GlobalPlatform TEE specifications. Hardware Tamper resistance is not a basic requirement of the TEE Protection Profile (although implementations may address this aspect). Furthermore, firmware update of the TEE itself is outside the scope of the TEE protection profile, but Trusted Application (TA) update is covered by TMF protection profile.

The assessment is linked to the current state of the GlobalPlatform specifications as referenced in Section 2. GlobalPlatform specifications generally provide detailed implementation parameters and have corresponding protection profiles so that a baseline in portability of services is achieved. Often, the GlobalPlatform specifications are more constraining than the SAE J3101 requirements definition.

3.2 Interpreting Coverage Analysis

This document aims to provide an overview of the coverage of the different SAE J3101 requirements by GlobalPlatform specifications for Secure Elements and Trusted Execution Environment. The purpose is to highlight those requirements that are currently covered and to identify any gaps that require additional support or may be covered in the future.

The result of the analysis summarizes GlobalPlatform technologies explicitly and fully satisfy SAE J3101 requirements for:

- 81% by Certified Secure Element Products
- 76% by Certified Trusted Execution Environment Products

An additional segment of satisfying requirements is met by 19% for Secure elements and 22% for Trusted Execution Environments by the development of specific Trusted Applet/Application running on a GlobalPlatform compliant platform.

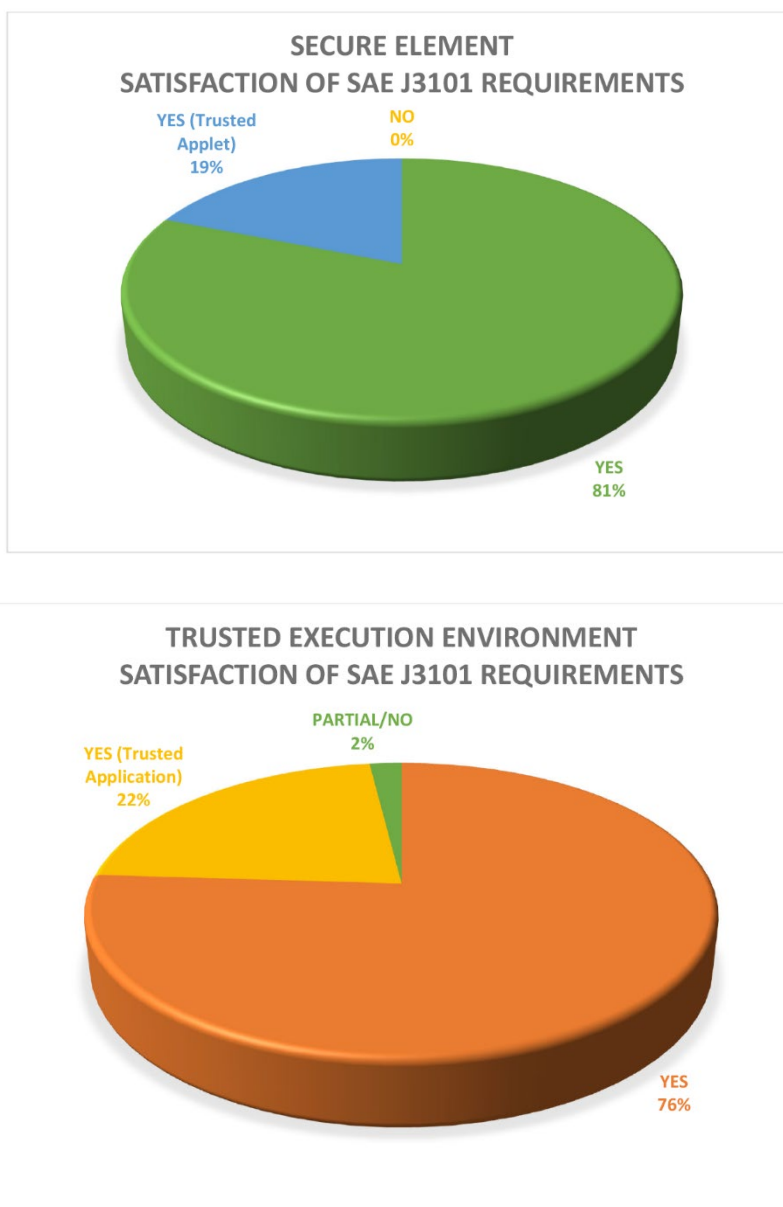


Figure 1 - Percentage of fulfilment of SAE J3101 requirements by GlobalPlatform technologies (mandatory and optional requirements)

3.2.1 Interpreting Non-Covered Requirements

There are three SAE J3101 requirements that are not fully met by GlobalPlatform TEE specifications. Hardware Tamper resistance is not a basic requirement of the TEE Protection Profile (although implementations may address this aspect). Furthermore, firmware update of the TEE itself is outside the scope of the TEE protection profile, but Trusted Application (TA) update is covered by TMF protection profile.

4. MAPPING OF GLOBALPLATFORM TECHNOLOGY SUPPORT WITH COMMENTS

Requirement ID	Condition	Requirement Description	SE Supported	SE Mapping	TEE Supported	TEE Mapping
<i>Types of Keys</i>						
REQ_6.2.3.1_10:	[MANDATORY]	The hardware protected security environment shall support digital certificates if public keys (asymmetric cryptography) are employed. The digital certificates should be X.509 or IEEE 1609.2 compatible formats.	Yes (TA)	X.509 is supported. IEEE 1609.2 is supported through an Application/Configuration.	Yes (TA)	X.509 is supported. IEEE 1609.2 is supported through an Application/Configuration.
REQ_6.2.3.1_20:	[OPTIONAL]	The hardware protected security environment shall support either ephemeral or long-term symmetric keys, or both.	YES		YES	
<i>Key Storage</i>						
REQ_6.2.3.2_10:	[MANDATORY]	A hardware protected security environment must securely store all cryptographic keys and explicitly control access to each.	YES	Mandated by [SE PP].	YES	Mandated by [TEE PP].
REQ_6.2.3.2_20:	[MANDATORY]	A keystore may be direct storage of the keys within the hardware protected security environment, or use of external storage external to the hardware protected security environment that is protected by encryption and integrity mechanisms implemented within the hardware protected security environment.	YES		YES	Mandated by [TEE PP].
REQ_6.2.3.2_30:	[OPTIONAL]	Key storage capacities should only be constrained by the physical limits of the underlying hardware. Allocation of storage between differing uses should be defined under each application specified for the hardware protected security environment, both in maximums and minimums. Denial of service due to exhaustion of available resources should be mitigated by a resource manager implemented in either hardware or firmware as a part of the hardware protected security environment.	YES	The SE PP mandates the physical limit of memory storage. In the GP API, there is a mechanism for Granted Memory per memory type in the installation/registry to avoid DoS.	YES	The TEE PP mandates the physical limit of memory storage. In the TEE Core API, there is a mechanism for Memory Allocation per memory type in the installation/registry to avoid DoS.
REQ_6.2.3.2_40:	[MANDATORY]	The hardware protected security environment keystore and its cryptographic key contents shall be separately managed from any other nonvolatile data protection. This includes other nonvolatile data both within the hardware protected security environment and in the normal environment.	YES	Segmentation of key storage is done via the security domain. The SE PP covers segmentation, protection, and integrity as requirements for TOE.	YES	Segmentation of key storage is done via the security domain.
REQ_6.2.3.2_50:	[MANDATORY]	The hardware protected security environment shall distinctly manage the cryptographic integrity of the keystore from other components of the hardware protected security environment.	YES	Mandated by [SE PP].	YES	Mandated by [TEE PP].
REQ_6.2.3.2_60:	[MANDATORY]	The hardware protected security environment shall manage and maintain the integrity of the entire keystore during any updates to the keystore (addition, modification, or deletion of a key).	YES	Mandated by [SE PP].	YES	Mandated by [TEE PP].
REQ_6.2.3.2_70:	[MANDATORY]	The hardware protected security environment shall check the integrity of the keystore before any transaction which makes use of a stored key, as well as in response to any conditions that warrant a check of the integrity of the keystore specified by the system design (e.g., normal or abnormal changes to power mode).	YES	Mandated by GlobalPlatform SE specifications (https://globalplatform.org/specs-library/?filter-committee=se) and [SE PP].	YES	Mandated by [TEE Config] and [TEE PP].

Requirement ID	Condition	Requirement Description	SE Supported	SE Mapping	TEE Supported	TEE Mapping
REQ_6.2.3.2_100:	[MANDATORY]	The hardware protected security environment keystore shall maintain the identification and association of each cryptographic key to its authorized calling application (called key-entity association), whether the application is located internal or external to the hardware protected security environment and whether the key is stored within or outside the protected hardware protected security environment boundary.	YES	Part of Security Domain/application Keys management Mandated by [SE PP].	YES	Mandated by [TEE Config] and [TEE PP] compliance for internal applications (TAs).
REQ_6.2.3.2_110:	[MANDATORY]	The hardware protected security environment shall maintain the hierarchy and/or association of all cryptographic keys within the keystore that are protected by other stored cryptographic keys.	YES	Part of Security Domain/application Keys management Mandated by [SE PP].	YES	Mandated by [TEE Config] and [TEE PP].
REQ_6.2.3.2_130:	[MANDATORY]	All cryptographic keys stored encrypted within the keystore (internal or external to the hardware protected security environment secure boundary) shall be encrypted by a cryptographic algorithm and key length combination that results in a computational resistance to attack equal to or greater than the stored key.	YES	Part of Security Domain/application Keys management Mandated by [SE PP].	YES	Mandate by [TEE PP] in combination with [Crypto Rec] as this is guidance for lab evaluation.
REQ_6.2.3.2_140:	[OPTIONAL]	If the encryption mode used to encrypt any internally or externally stored key requires an initialization vector, such shall be distinct in each key encryption operation.	YES	Part of Security Domain/application Keys management Mandated by [SE PP].	YES	Mandated as part of [TEE PP].
REQ_6.2.3.2_150:	[MANDATORY]	The hardware protected security environment shall support binding of keys that are stored encrypted within the keystore to a specific device.	YES	Part of Security Domain/application Keys management Mandated by [SE PP].	YES	Mandated by [TEE Config] and [TEE PP].
<i>Long-Term Keying Material Protection</i>						
REQ_6.2.3.2.1_10:	[MANDATORY]	Long-term keys must be protected while at rest for confidentiality, integrity, and against replay attacks. These attacks could be mounted on the nonvolatile storage device containing these keys or in transit from the nonvolatile storage device to the security module if the security module does not contain on-board nonvolatile storage.	YES	Part of Security Domain/application Keys management Mandated by [SE PP].	YES	Mandated by [TEE Config] and [TEE PP].
<i>Short-Term Keying Material Protection</i>						
REQ_6.2.3.2.2_20:	[MANDATORY]	The hardware protected security environment shall protect the confidentiality and integrity of short-term keys used on a session basis while in transit (during key exchange operations) and against replay attacks.	YES	Part of Security Domain/application Keys management Mandated by [SE PP]. All Keys are stored within the TOE.	YES	Mandated by [TEE Config] and [TEE PP].
REQ_6.2.3.2.2_30:	[MANDATORY]	The hardware protected security environment shall ensure that the exposure of any short-term keys used on a session basis does not compromise the integrity and confidentiality of any other short-term keys used in past or future sessions.	YES	Part of Security Domain/application Keys management	YES	[TEE Config] RNG aspect Mandated by [TEE PP].
REQ_6.2.3.2.2_10:	[OPTIONAL]	The hardware protected security environment shall protect short-term keys used on a session basis such that at the termination of that session their use is also terminated.	YES	Transient keys are automatically deleted at card reset or applet deselection.	YES	Supported by the [TEE Core] 4.5 Trusted Application Configuration Properties.

Requirement ID	Condition	Requirement Description	SE Supported	SE Mapping	TEE Supported	TEE Mapping
<i>Symmetric Key Protected Storage</i>						
REQ_6.2.3.2.3_10:	[MANDATORY]	Symmetric keys (also referred to as shared secret keys) shall be preserved for integrity, confidentiality, and freshness.	YES	Part of Security Domain/application Keys management.	YES	Mandated by [TEE Config] and [TEE PP].
REQ_6.2.3.2.3_20:	[OPTIONAL]	The hardware protected security environment shall encrypt internally stored symmetric keys using an internally stored key encryption key.	YES	Part of Security Domain/application Keys management. Mandated by [SE PP]. All Keys are stored within the TOE.	YES	Mandated by [TEE Config] and [TEE PP].
REQ_6.2.3.2.3_30:	[MANDATORY]	The hardware protected security environment shall output externally stored symmetric keys by a method that meets the key output requirements of this document.	YES	Part of Security Domain/application Keys management. Mandated by [SE PP]. All Keys are stored within the TOE.	YES	
REQ_6.2.3.2.3_50:	[OPTIONAL]	The hardware protected security environment shall support a defined lifetime and a means of rekeying for symmetric keys.	Yes (TA)	To be managed on a per applet level.	Yes (TA)	Supported through an Application (TA)/Configuration.
<i>Asymmetric Key Protected Storage</i>						
REQ_6.2.3.2.4_10:	[MANDATORY]	The hardware protected security environment shall protect public keys by using the hardware protected security environment's facilities for integrity to prevent unauthorized modification or substitution or rollback.	YES	Mandated by [SE PP].	YES	Mandated by [TEE Config] and [TEE PP].
REQ_6.2.3.2.4_15:	[MANDATORY]	For confidentiality, the hardware protected security environment shall store and use private keys strictly inside the hardware protected security environment for confidentiality, i.e., to prevent any unauthorized disclosure of the private key outside the environment.	YES	By default, everything is protected.	YES	By default, everything is protected.
REQ_6.2.3.2.4_20:	[MANDATORY]	The hardware protected security environment shall maintain the associations of all private keys with their respective public keys.	YES	Part of Security Domain/application Keys management.	YES	Mandated by [TEE Config] and [TEE PP].
<i>Protection at Use</i>						
		Secure Key Usage: Secure key usage pertains to a hardware protected security environment controlling the use (execute privileges) of a cryptographic key by a specific entity (application) for a specific purpose. An API is assumed to be required through which applications outside of the hardware protected security environment can distinctly manage and use the keystore without unauthorized disclosure of its keys. Secure key usage pertains to the key store APIs and the authorization to access the keys and control their usage.				
REQ_6.2.3.3_10:	[MANDATORY]	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	By design.	YES	Supported through the TEE Core API. Mandated by [TEE Config] and [TEE PP].
REQ_6.2.3.3_20:	[MANDATORY]	The hardware protected security environment shall maintain the security of all cryptographic algorithm keys during their use.	YES	Done by the firewall from the Run time environment. Mandated by [SE PP].	YES	Mandated by [TEE Config] and [TEE PP].