Certification Report

TrustWare 3.0 (v3.0.5)

Sponsor and developer: ***Samsung Electronics Co., Ltd.***
129 Samsung-ro, Yeonggtong-gu,
Suwon-si, Gyeonggi-do, 443-742
Korea

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-234008-CR**

Report version: **1**

Project number: **234008**

Author(s): **Denise Cater**

Date: **9 October 2019**

Number of pages: **13**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5 (ISO/IEC 15408)
Certificate number	**CC-19-234008**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Samsung Electronics Co., Ltd.** **129 Samsung-ro, Yeonggtong-gu, Suwon-si, Gyeonggi-do, 443-742, Korea**
Product and assurance level	**TrustWare 3.0 (v3.0.5)** Assurance Package: ▪ EAL2 augmented AVA_TEE.2
Project number	**234008**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5 (ISO/IEC 18045)

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 5 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 5. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS Mutual Recognition Agreement for components up to EAL4

Validity	Date of 1st issue : 11-**10-2019** Certificate expiry : 11-**10-2024**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the (site) security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.eIDAS-Regulation

TÜV Rheinland Nederland BV, operating the Netherlands Scheme for Certification in the Area of IT Security (NSCIB), has been notified as a Designated Certification Body from The Netherlands under Article 30(2) and 39(2) of Regulation 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the TrustWare 3.0 (v3.0.5). The developer of the TrustWare 3.0 (v3.0.5) is Samsung Electronics Co., Ltd. located in Gyeonggi-do, Korea and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE, TrustWare 3.0 (version 3.0.5), is the Trusted OS part of a Trusted Execution Environment (TEE) for embedded devices implementing GlobalPlatform TEE specifications (TEE System Architecture *[SA]*, TEE Internal API *[IAPI]* and TEE Client API *[CAPI]*).

The TOE supports the implementation of an execution environment isolated from any other execution environment, including the usual Rich Execution Environment (REE), and their applications. Once integrated into a TEE, the TOE hosts a set of Trusted Applications (TA) and provides them with a comprehensive set of security services including: integrity of execution, secure communication with the Client Applications (CA) running in the REE, trusted storage, key management and cryptographic algorithms, time management and arithmetical API.

The TOE comprises:

- The trusted OS part of a TEE solution
- The guidance for the secure usage of the TEE OS functionality after delivery.
- The guidance for the integration of the TOE into a TEE solution.

The TOE does not comprise:

- The Trusted Applications
- The Rich Execution Environment (REE)
- The Client Applications
- The underlying platform (hardware and firmware)

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 9 October 2019 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the TrustWare 3.0 (v3.0.5), the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the TrustWare 3.0 (v3.0.5) are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provides sufficient evidence that the TOE meets the EAL2 augmented (EAL2(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with AVA_TEE.2 (Low TEE vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the TrustWare 3.0 (v3.0.5) from Samsung Electronics Co., Ltd. located in Gyeonggi-do, Korea.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	TrustWare 3.0	v3.0.5

To ensure secure usage a set of guidance documents is provided together with the TrustWare 3.0 (v3.0.5). Details can be found in section "Documentation" of this report.

2.2 Security Policy

The TOE has the following features:

- Isolation of the TEE services, the TEE resources involved and all the Trusted Applications from the REE
- Isolation between Trusted Applications and isolation of the TEE from Trusted Applications
- Protected communication interface between CAs and TAs within the TEE, including communication endpoints in the TEE
- Trusted storage of TA and TEE data and keys, ensuring consistency, confidentiality, atomicity and binding to the TEE
- Random Number Generator
- Cryptographic API including:
  - Generation and derivation of keys and key pairs
  - Support for cryptographic algorithms as described in the table below
- TA instantiation that ensures the authenticity and contributes to the integrity of the TA code
- Correct execution of TA services

Cryptographic Operation	Cryptographic Algorithm	Supported key sizes	Corresponding Standards
Symmetric Cipher	AES (ECB, CBC, CTR, XTS, CCM, GCM)	128, 192, 256[2]	FIPS 197 (AES) NIST SP800-38A (ECB, CBC, CTR) IEEE Std 1619-2007 (XTS) RFC 3610 (CCM) NIST 800-38D (GCM)
	DES, TDES (ECB, CBC)	56, 112, 168	FIPS 46 (DES, 3DES) FIPS 81 (ECB, CBC)
Digest	MD5, SHA1, SHA224, SHA256, SHA384, SHA512	Not applicable	RFC 1321 (MD5) FIPS 180-4 (SHA1 SHA224 SHA256 SHA384 SHA512)

[2] XTS only supports key sizes 128 and 256 bits

Cryptographic Operation	Cryptographic Algorithm	Supported key sizes	Corresponding Standards
MAC	AES (CMAC, CBC MAC)	128, 192, 256	NIST SP800-38B (CMAC) ISO9797 (CBC MAC)
	DES, TDES (PKCS5, CBC MAC)	56, 112, 168	ISO9797 RFC1423
	HMAC (MD5, SHA1, SHA224, SHA256, SHA384, SHA512)	Limited by the block size of the hash function	RFC 2202 (MD5, SHA1) RFC 4231 (SHA224 SHA256 SHA384 SHA512)
Asymmetric Cipher	RSAES (without padding, PKCS#1 v1.5, OAEP)	256, 512, 768, 1024, 1536, 2048, 3072	PKCS#1
Digital Signature	RSASSA (without padding, PKCS#1 v1.5, PSS)	256, 512, 768, 1024, 1536, 2048, 3072	PKCS#1
	DSA	Depends on Algorithm: TEE_ALG_DSA_SHA1 : Between 512 and 1024 bits, multiple of 64 bits TEE_ALG_DSA_SHA224 : 2048 bits TEE_ALG_DSA_SHA256 : 2048 or 3072 bits	FIPS 186-4
	ECDSA	160, 192, 224, 256, 384, 521	FIPS 186-4 ANSI X9.62
	ED25519	256	RFC 8032 RFC 7748
Key Exchange (Shared secret derivation)	DH	From 256 to 2048 bits, multiple of 8 bits.	PKCS #3
	ECDH	192, 224, 256, 384, 521	NIST SP800-56A
	X25519	256	RFC 7748

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

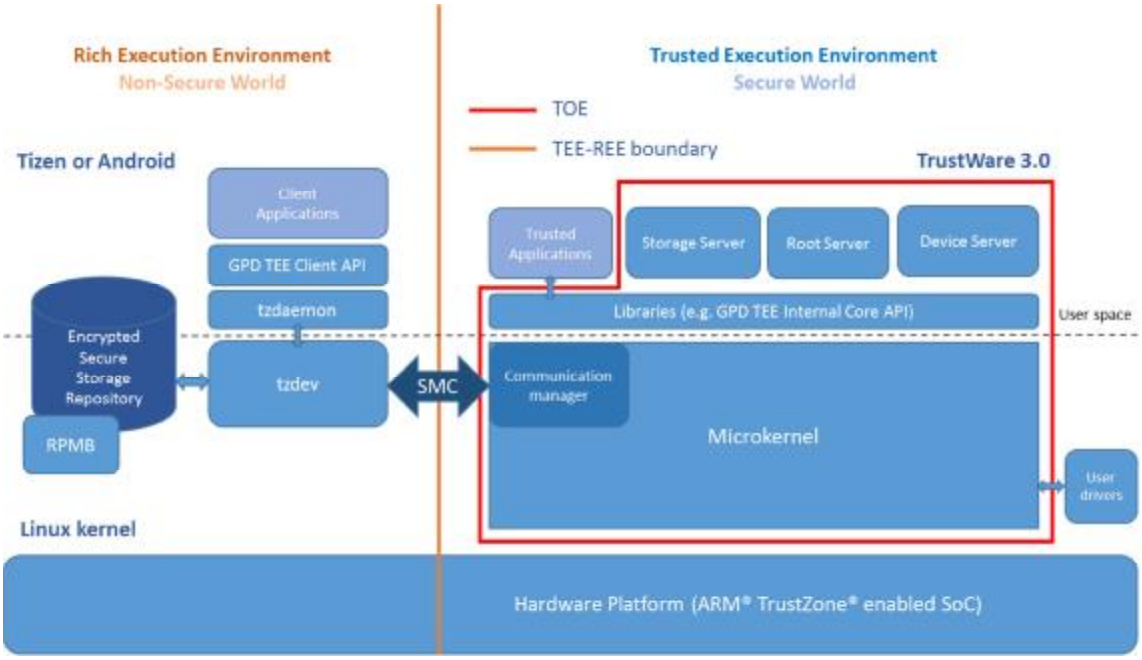
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

2.3.2 Clarification of scope

The TOE is a software Trusted Execution Environment that relies on the underlying hardware and firmware to fulfil the objective OE.SECURE_ENVIORNMENT as described to [ST] section 4.2.

2.4 Architectural Information

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows



2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
TrustWare 3.0 Certified Product Guidance	1.10, September 05, 2019
TrustWare 3.0 Internal Driver API	1.4, July 8, 2019
TrustWare 3.0 List of Secure Monitor Calls	1.4, August 22, 2019
TrustWare 3.0 Operational User Guidance	1.7, August 22, 2019
TrustWare 3.0 Preoperative Procedures	1.7, August 22, 2019
TrustWare 3.0 TA SDK User Manual	1.15, April 3, 2019
TrustWare 3.0 TEE API Extensions	1.4, July 8, 2019
TrustWare 3.0 User-Space Drivers	1.3, July 8, 2019
TrustWare 3.0 Driver Porting Guide	1.3, July 8, 2019
TrustWare 3.0 Compilation Guide	1.4, July 9, 2019
TrustWare 3.0 Installation Guide	1.3, July 9, 2019

2.6 IT Product Testing

Testing (coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach

The developer has performed extensive testing against the functional specification and divided their test effort in different test groups, each focusing on different parts of the TOE functionality and

covering the different TSFIs. The testing was automated using industry standard and proprietary test suites. Test scripts were extensively used to verify that the functions return the expected values.

For the testing performed by the evaluators, the developer has provided a test environment. The evaluators have reproduced the entire developer test suite, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent Penetration Testing

To identify potential vulnerabilities, the evaluator performed the following activities:

- SFR design analysis: SFR implementation details were examined in the SFR design analysis. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check was performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.
- CWE vulnerability focus: Using the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. This approach ensured that the evaluator was forced to think in terms of vulnerabilities from all different angles and improved completeness in the vulnerability analysis. Also during this examination several potential vulnerabilities were identified.
- Public vulnerability search: Several additional potential vulnerabilities were identified during a search in the public domain.
- A judgment was made on how to assure that these potential vulnerabilities are not exploitable. For most of the potential vulnerabilities a penetration test was defined. It was concluded that some potential vulnerabilities were not applicable or were covered by guidance.

The distribution of the different test categories is as follows.

Penetration test category	% of total number of penetration tests
Reverse engineering	10%
Interface fuzzing/abuse	30%
Memory manipulation	20%
Logging	10%
Malformed ELF	10%
UUID impersonation	10%
RAM file system	10%
Total:	**100% (10 tests)**

2.6.3 Test Configuration

The TOE version used by the developer and by the evaluator for the repeat of the developer testing was TrustWare 3.0 v3.0.5.

For all testing TOE was tested using the hardware configuration: Muse-M board equipped with sdp1803 DTV SoC and a secure bootloader.

The TOE version used for the penetration testing was TrustWare 3.0 v3.0.4 for all test cases. The results of one test case executed on TOE version v3.0.4 resulted in a new updated TOE version v3.0.5. Therefore, this test case was repeated with the updated TOE TrustWare 3.0 v3.0.5 to assess the impact of the changes. Other test cases were concluded to not be impacted by the code changes.

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its *[ST]* and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number TrustWare 3.0 (v3.0.5).

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references a ASE Intermediate Report and other evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the TrustWare 3.0 (v3.0.5), to be **CC Part 2 extended, CC Part 3 extended**, and to meet the requirements of **EAL 2 augmented AVA_TEE.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation.

3 Security Target

The Samsung TrustWare 3.0 (v3.0.5) Security Target, version 1.0, September 5, 2019 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

CWE	Common Weakness Enumeration
ELF	Executable and Linkable Format
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
NSCIB	Netherlands Scheme for Certification in the area of IT security
PP	Protection Profile
RAM	Random Access Memory
REE	Rich Execution Environment
TEE	Trusted Execution Environment
TOE	Target of Evaluation
UUID	Universally Unique Identifier

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CAPI]	TEE Client API Specification, GlobalPlatform (Version 1.0, July 2010, ref: GPD_SPE_007)
[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
[ETR]	Evaluation Technical Report TrustWare 3.0 (v3.0.5), 19-RPT-594, Version 1.1, 05 September 2019.
[IAPI]	TEE Internal API Specification, GlobalPlatform (Version v.1.1.2, November 2016, ref: GPD_SPE_010)
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[SA]	TEE System Architecture, GlobalPlatform (Version 1.1, January 2017, ref: GPD_SPE_009)
[ST]	Samsung TrustWare 3.0 (v3.0.5) Security Target, version 1.0, September 5, 2019.

(This is the end of this report).