Certification Report

Qualcomm® Trusted Execution Environment (TEE) v5.8 on Qualcomm® Snapdragon™ 865

Sponsor and developer:	***Qualcomm Technologies, Inc.*** **5775 Morehouse Drive** **CA 92121 San Diego** **U.S.A.**
Evaluation facility:	***Riscure B.V.*** **Delftechpark 49** **2628 XJ Delft** **The Netherlands**
Report number:	**NSCIB-CC-0244671-CR**
Report version:	**1**
Project number:	**0244671**
Author(s):	**Denise Cater**
Date:	**03 August 2021**
Number of pages:	**12**
Number of appendices:	**0**

Head Office:
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 Netherlands Chamber of Commerce (KVK), under number 27288788.

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

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 licence 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, 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

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Qualcomm® Trusted Execution Environment (TEE) v5.8 on Qualcomm® Snapdragon™ 865. The developer of the Qualcomm TEE v5.8 on Snapdragon 865 is Qualcomm Technologies, Inc. located in San Diego, USA 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 is a trusted execution environment (TEE) which is intended to operate in parallel to a rich execution environment (REE). It allows for executing trusted applications (TAs) in a secured manner isolated from any applications running in REE. The TEE is integrated into a system-on-chip (SoC) and utilizes hardware components of the SoC as outlined in more detail in the description of the physical scope of the TOE.

The TOE offers a comprehensive set of services to the TAs including integrity of execution, secure communication with the client applications (CA) running in REE, trusted storage, key management and cryptographic algorithms, time management, and arithmetical application programming interfaces (API).

The TOE is an open environment where TAs can be loaded and installed post-issuance (in the end user phase of the TEE-enabled device).

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 02 August 2021 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 Qualcomm® Trusted Execution Environment (TEE) v5.8 on Qualcomm® Snapdragon™ 865, 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 Qualcomm TEE v5.8 on Snapdragon 865 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 provide 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 (Vulnerability Analysis of TEE.

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]* (Parts I, II and III).

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. Note that the certification results apply only 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 available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Qualcomm TEE v5.8 on Snapdragon 865 from Qualcomm Technologies, Inc. located in San Diego, USA.

The TOE is comprised of the components:

Delivery item type	Identifier	Version
Hardware	SM8250 Hardware	TCSR_SOC_HW_VERSION register (0x60080201) 0x6080 – chip family ID 0201 – version 2.1
Hardware	SM8250 ROM Code containing the Primary Bootloader (PBL)	TCSR_SOC_HW_VERSION register
QTI signed Binary Load Images	Qualcomm TEE kernel v5.8, CommonLib (tz.mbn)	TZ.XF.5.8-00041.3-SM8250AAAAANAZT-3
QTI signed binary image.	XBL-SEC xbl_sec.mbn	BOOT.XF.3.2-00295-SM8250-1
Library intended to be statically linked into TAs	applib.lib - 32 bit applib.lib - 64 bit common_applib.o - 32bit common_applib.o - 64bit	TZ.APPS.1.8.c1-00005-SM8250AAAAANAZT-1
Binary Load Images	Mandatory QTI System TAs	As specified in [ST] section 2.3.3
Attestation(Binary file)	qwes.mbn	TZ.APPS.1.8.c1-00005-SM8250AAAAANAZT-1
eSE (Binary file)	eseservice.mbn SCP11cry.mbn tee_se_api.lib	TZ.APPS.1.8.c1-00005-SM8250AAAAANAZT-1

To ensure secure usage a set of guidance documents is provided, together with the Qualcomm TEE v5.8 on Snapdragon 865. For details, see section 2.5 “Documentation” of this report.

2.2 Security Policy

The TOE overview describes the following major security features of the TOE. The TOE consists of a secure execution environment implemented in software and executing on a System on Chip (SoC). The secure execution environment operates in a hardware enforced isolation of the rich execution environment. The system consists of the following main components:

- Secure boot mechanism in which the hardware-based root of trust uses cryptographically strong signature verification over the software components loaded for secure initialisation of the TOE hardware, QTEE and REE.
- QTEE v5.8 the secure execution environment and common services layer provided to TAs.
- GlobalPlatform TEE API support for trusted applications.

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. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 6.1.1 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The TOE depends on the following non-TOE hardware components for proper functioning:

- External dynamic random-access memory (DRAM, either external or deployed as package-on-package).
- Replay protected memory block (RPMB, to support secure file system (SFS) version and TrustZone applications version anti-rollback).

The OEM is responsible for communicating the proper use of the integrated device to the final TEE users. This guidance might not be a document but a commercial notice. The OEM provides an explanation if there is no action or behaviour expected from the TEE final user.

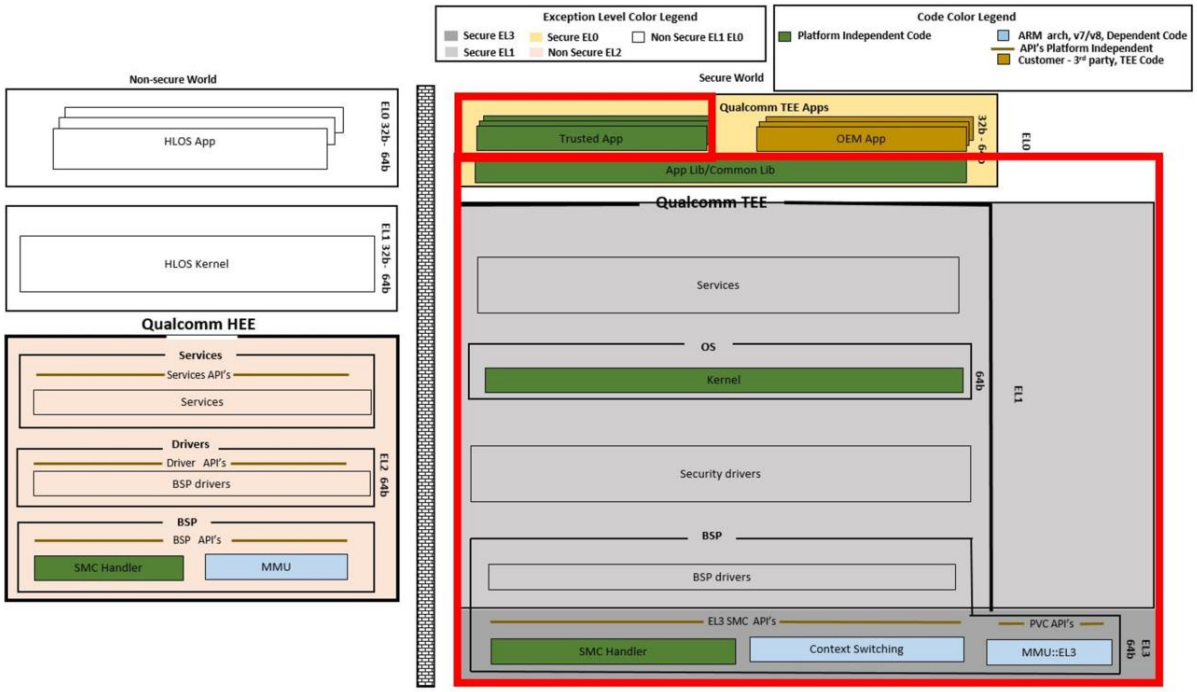
2.4 Architectural Information

The TOE is a trusted execution environment (TEE) which is intended to operate in parallel to a rich execution environment (REE). It allows for executing trusted applications (TA) in a secured manner isolated from any applications running in REE. The TEE is integrated into a system-on-chip (SoC) and utilizes hardware components of the SoC as outlined in more detail in the description of the physical scope of the TOE.

The TOE offers a comprehensive set of services to the TAs including integrity of execution, secure communication with the client applications (CA) running in REE, trusted storage, key management and cryptographic algorithms, time management, and arithmetical application programming interfaces (API).

The TOE is an open environment where TAs can be loaded and installed post-issuance (in the end user phase of the TEE-enabled device).

The TOE also incorporates the Qualcomm Hypervisor Execution Environment (Qualcomm HEE) component that seamlessly interacts with the TEE to manage resources shared between the REE and the TEE. The QHEE operates with the highest (hypervisor) privileges (EL2) within the REE.



Qualcomm TEE v5.8 provides application programming interfaces to the TAs and a communication interface to REE. In addition to this, the system offers debugging interfaces, but the OEM must effectively disable these debugging interfaces in the secure operational configuration of the product.

The TOE provides also functionality to the TAs to establish a trusted path to an embedded secure element (eSE). The eSE itself is not part of the TOE.

Finally, the TOE provides the functionality to support device attestation of the TEE.

2.5 Documentation

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

Guidance for SoC integrators:

Identifier	Version
SM8250 Security Overview (80-PK882-10)	Rev C
SM8250 Secure Boot Enablement User Guide (80-PK882-9)	Rev B
Debug Policy Version 2 User Guide (80-NV396-72)	Rev E
Provisioning Encryption Tool User Guide (80-P1824-1)	Rev B
SM8250 QFPROM Programming Reference Guide (80-PL546-97)	Rev B
Sectools: FuseBlower Tool User Guide (80-NM248-3)	Rev K
Sectools: SecImage Tool (Version 5.20 and Later) User Guide (80-NM248-8)	Rev C
Sectools: KeyProvision Tool User Guide (80-NM248-5)	Rev B
Sectools: Debug Policy Tool User Guide (80-NM248-6)	Rev K
Security Quick Start (80-PF777-103)	Rev J
TEE-based Mobile Payment Security Guidelines for OEMs (80-NR875-15)	Rev J
SM8250+SDX55M Software User Manual (SP80-PK882-4)	Rev G
SM8250 Linux Peripheral (UART, SPI, I2C, I3C) Overview (80-PK882-6)	Rev C
Secure Channel Protocol 11 Configuration Guide (80-P2484-142)	Rev A
KBA-191027204619, eSE enablement	Rev 7
AGD_PRE: Qualcomm® Trusted Execution Environment (TEE) Product Delivery User Guide (80-NR875-20, June 17, 2021)	Rev AA

Guidance for TA developers:

Identifier	Version
Secure Coding Guidelines for TrustZone QTEE Applications (80-NK069-1)	Rev A
Qualcomm TEE Reference Manual (80-NH537-4)	Rev K
Qualcomm TEE TA Software Developers Kit (80-PF777-58)	Rev A
Qualcomm WES API Reference (80-PL230-2)	Rev H

2.6 IT Product Testing

Testing (depth, 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 and depth

The developer has performed extensive testing on functional specification and TSFIs. The testing was largely 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 provided samples and a test environment. The evaluators reproduced a selection of the developer tests. No independent functional tests were generated because the evaluator did not identify any gaps in the developer test campaign that needed to be addressed through evaluator independent functional tests.

2.6.2 Independent penetration testing

The TOE is a TEE. Therefore, the vulnerability analysis is performed based on the structure of the attack methods defined by *[GP_TEE]*. For each attack method, the objective of the attack and how the attack method applies to the TOE is described. The following is considered for each attack method:

- Collect and review information available in the public domain.
- Collect and review information and prior work of the security evaluation facility.
- Determine viable attack scenarios based on available information.
- Select attacks for the penetration testing phase.

Based on these items, it was determined whether an attack method is applicable to the TOE and should be tested during the penetration testing phase.

The vulnerability analysis took information from the design assessment of the TOE into account. However, an EAL2 evaluation is more explorative in nature than a full white-box evaluation where also implementation details and source code is available for inspection, so specific emphasis was placed upon the information gathering activities.

The attack methods specified in *[GP_TEE]* were also considered.

To rate the difficulties to exploit potential vulnerabilities the evaluation uses the standard rating methodology from *[CC]* and from the GP PP *[GP_TEE]*.

The total test effort expended by the evaluators was 15 days. During that test campaign, 100% of the total time was spent on side-channel testing.

2.6.3 Test configuration

The configuration of the sample used for independent evaluator penetration testing was the same as described in the *[ST]*. Having confirmed the differences between the 32bit and 64bit libraries were not security relevant, the 64bit libraries were used by the evaluator for testing.

2.6.4 Test 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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN.2/AVA_TEE.2 activities. No exploitable vulnerabilities were found within the capabilities of an attacker with basic/TEE-Low attack potential

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Reused Evaluation Results

There is no reuse of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Qualcomm® Trusted Execution Environment (TEE) v5.8 on Qualcomm® Snapdragon™ 865.

2.9 Evaluation Results

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other evaluator documents. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that must be considered when this TOE is used as platform in a composite evaluation.

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

Based on the above evaluation results the evaluation lab concluded the Qualcomm TEE v5.8 on Snapdragon 865, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 2 augmented with AVA_TEE.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

The Security Target claims 'strict' conformance to the Protection Profile *[GP_TEE]*., including the PP modules TEE TIME AND ROLLBACK and TEE DEBUG.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE. However, the OEM is responsible for communicating the proper use of the integrated device to the final TEE users. This guidance might not be a document but a commercial notice. The OEM provides an explanation if there is no action or behaviour expected from the TEE final user.

In addition, all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself must 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. For the evolution of attack methods and techniques to be covered, the customer 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. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: None.

The security strength of cryptographic mechanisms was out of the scope of this evaluation.

3 Security Target

The Qualcomm® Trusted Execution Environment (TEE) v5.8 on Qualcomm® Snapdragon™ 865 Security Target, 80-NR875-18, Rev. AA, July 20, 2021 *[ST]* is included here by reference.

Please note that, to satisfy the need for publication, a public version *[ST-lite]* has been created and verified according to *[ST-SAN]*.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

API	Application Programming Interfaces
CA	Client Application
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
QTEE	Qualcomm® Trusted Execution Environment
REE	Rich Execution Environment
SoC	System-On-Chip
TA	Trusted Application
TEE	Trusted Execution Environment
TOE	Target of Evaluation

5 Bibliography

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

[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 for Qualcomm TEE v 5.8 on Snapdragon 865, Document ID 1930093-D3, v1.8, 29 July2021
[ETRfC]	ETR for composite evaluation for Qualcomm® Trusted Execution Environment (TEE) v5.8 on Qualcomm® Snapdragon™ 865, Document ID 1930093-D4, v1.7, 29 July 2021
[GP_TEE]	Global Platform Device Committee, TEE Protection Profile, GPD_SPE_021, V1.2.1, November 2016, registered under the reference ANSSI-CC-PP-2014/01-M01.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Qualcomm® Trusted Execution Environment (TEE) v5.8 on Qualcomm® Snapdragon™ 865 Security Target, 80-NR875-18, Rev. AA, July 20, 2021
[ST-lite]	Qualcomm® Trusted Execution Environment (TEE) v5.8 on Qualcomm® Snapdragon™ 865 Security Target Lite, 80-NR875-21, Rev. AA, July 20, 2021
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)