Certification Report

Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support

Sponsor and developer: ***Qualcomm Technologies Inc.***
5775 Morehouse Dr
San Diego, CA 92121
USA

Evaluation facility: ***Riscure B.V.***
Delftechpark 49
2628 XJ Delft
The Netherlands

Report number:	**NSCIB-CC-0227918-CR**
Report version:	**1**
Project number:	**0227918**
Author(s):	**Hans-Gerd Albertsen**
Date:	**02 December 2021**
Number of pages:	**15**
Number of appendices:	**0**

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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.

Reproduction of this report is authorised only if the report is reproduced in its entirety.

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 Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support. The developer of the Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support 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 system called the SPU serving as a Secure Element within a stacked DDR in PoP form factor on a SOC. It is designed as a tamper proof device providing secure storage and a secure execution environment for processing of sensitive data and for performing cryptographic operations using protected keys stored in its secure storage. Secure Elements can be used for multiple application areas that require a high level of security.

The TOE has dedicated interfaces to other components of the SOC, which allow those components to communicate with the TOE and request services from the TOE. The TOE is comprised of a hardware layer, and IC dedicated software providing interfaces for application developers.

The TOE is embedded onto Qualcomm® Snapdragon™ 888, used in mobile applications. Qualcomm® Snapdragon™ 888 comprises a high-level Operating system (HLOS, such as Android) and Trusted Execution Environment (TEE, such as QTEE v5) that are required for the TOE to boot and properly communicate with the rest of the Hardware and Software.

This TOE is critically dependent on the operational environment, namely the objective for the environment as defined in the *[ST]*, to provide countermeasures against specific attacks as described in section 2.3.1 of the user guidance 80-NH537-4 Rev.M as referenced in the ST.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 02 December 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 Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support, 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 Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support 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 EAL4 augmented (EAL4+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical 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]* (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 Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support from Qualcomm Technologies Inc. located in San Diego, USA.

The TOE is comprised of the following main components:

Delivery item type	**Identifier**	**Version**
Hardware	SPU 250 Hardware (HW version from RTL (Hardcoded)	4.1
Software	SPU firmware (PBL & Mission ROM) Foundry ID Samsung “S3“ Foundry ID Samsung “S5”	55100000 551000F2 551000F6
Software	SPU software (MCP & System application (cryptoapp & asym_cryptoapp))	SPSS.A1.1.4-00108-LAHAINA.0-1

To ensure secure usage a set of guidance documents is provided, together with the Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support. For details, see section 2.5 “Documentation” of this report.

For a detailed and precise description of the TOE lifecycle, see the *[ST]*, Chapter 3.2.10.

2.2 Security Policy

The TOE maintains:

the integrity and confidentiality of code and data stored in its memories as defined in the *[ST]*.
the integrity, the correct operation and the confidentiality of security functionality provided by the TOE.

This is ensured by the construction of the TOE and its security functionality.

The major security features of the TOE are described in Section 2.3 of [ASE.ST], and are categorized as follows:

- Internal Security functions - functionality related to the security of the TOE itself, primarily implemented at the OS level for logical protection mechanisms, e.g.:
  - Access controls for memories,
  - Access controls for keys managed by hardware,
  - Secure boot and root of trust,
  - Protection of user data,
  - Secure loading and updating of software and applications.
  - Domain separation between applications executed by the TOE.
  - Anti-replay island and software freshness protection.

- Cryptographic services (API) - functionality related to the Cryptographic Management Unit, primarily for cryptographic operation security, e.g.:
  - Random number generation,
  - Symmetric and asymmetric cryptographic algorithms (TDES, AES, RSA, Elliptic Curves)
  - Secure key storage in Cryptographic Management Unit,
  - Secure key generation and zeroization,
  - Hashing functions (e.g. SHA-1, SHA-256, SHA-384, SHA-512).

- Physical protection - functionality related to the physical protection of the TOE, primarily related to mechanisms to counter physical attacks at a hardware level, e.g.:

- memory scrambling/encryption,
- FI/SCA countermeasures,
- sensors,
- integrity checking.
- PoP form factor.

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 5.4 of the *[ST]*.

2.3.2 Clarification of scope

The evaluation did reveal a threat to the TOE that is not countered by the evaluated security functions of the product but by the operational environment. The assumption A.Protect-Shared-Comp is addressed by the security objective on the operational environment OE.Protect-Shared-Comp which requires the TEE component to be configured to restrict access of non-TOE components to specific interfaces of TOE. Details are described in guidance document as listed in chapter 2.5.

The Security Target claims no conformance to a Protection Profile.

2.4 Architectural Information

The TOE design is composed of three subsystems, one Hardware subsystem and two subsystems covering the IC dedicated software. Details are included in following sections.

Hardware subsystems

The hardware design of the TOE, as specified in [CC_ADV] is decomposed into a single subsystem named HW subsystem that includes all the hardware components of the TOE, such as Central Processing Unit, Cryptographic Management Unit, External Memory Management Unit, SP-SC QFPROM Memory, RAM and ROM memories, Local Resource Manager, Timer and Watchdog, Processor Interconnect Bus and Anti-Replay Island. Figure 1 below provides details on the hardware subsystem structure.

The TOE HW subsystem is decomposed into various modules, presenting a further decomposition into up to two additional levels of sub-modules. The higher-level modules of the HW subsystem are the following:

- CPU: Main CPU module including a Hardened CPU, RAM and ROM modules both with integrity/encryption protections, interconnection Bus Matrix, and a Hardware SWAP assisted memory virtualization component.
- CPU LRM: A Local Resource Manager (LRM) module that includes an Alternating Step Generator (ASG) providing entropy source for countermeasures, a Parallel Alternating Step Generator (PASG), providing source of entropy accessible by HW, and a access control and functionality configuration registers for the module subcomponents.
- EMM: An External Memory Manager (EMM) giving access to SOC address space.
- CMU: A Cryptographic Management Unit (CMU) composed by a Random Number Generator (RNG), a cryptographic Key Table, a cryptographic command interface, hardware cryptographic engines providing support for symmetric and hash cryptography, and a Public Key Engine (PKE) component providing support for asymmetric cryptography.
- Security Control: Providing controlled access to the SP-SC QFPROM memory.
- Anti-Replay Island: An Anti-Replay controller and Always-on timer.
- DMA: A Direct Memory Access (DMA) unit.
- Clock Controller: It includes a cold boot sequencer, a reset sequencer, clock generation for the SPU, and a Resource State Coordinator Complex (RSCC).
- Interconnect: A main interconnect module, including the SPU high-speed interconnect Network on Chip (NoC) and a clock domain crossing components for interconnect.

- CX LRM: It provides SPU interrupt mappings, routing and masking unit, and configuration for sensors used for detecting abnormal design behaviour and attacks.
- Debug module: Including an Input Output (IO) mux that blocks all debug and test features, a debug management core and a direct debug interface to SC300.
- Timers: A hardware module that provides independent timing and watchdog to the SPU.

Overall, the hardware subsystems define the whole hardware part of the TOE, identify the TSF, and show how the various subsystems interact which each other.

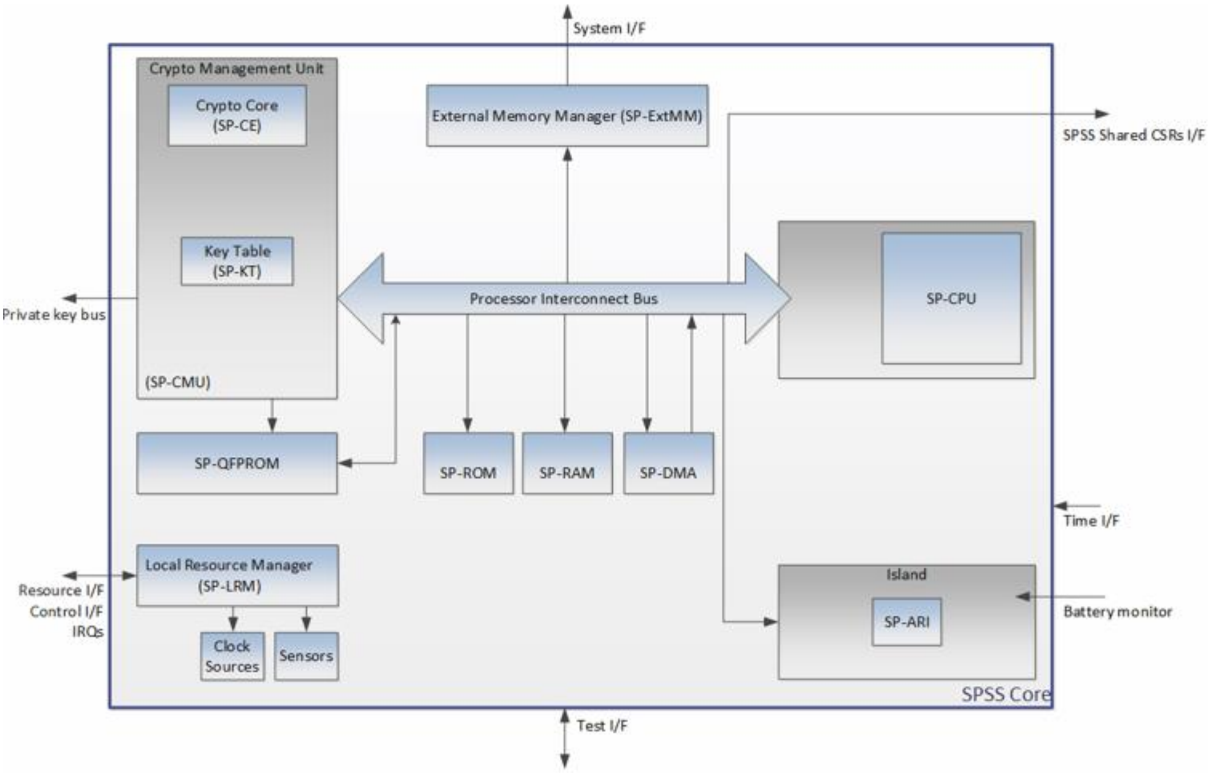

Figure 1: TOE hardware design decomposition

IC dedicated software subsystems

IC Dedicated Software comprises the SPU Firmware and SPU Software as described in Section 3.2.1 of the *[ST]*. The logical design decomposition of the IC Dedicated Software into two subsystems is as follows:

PBL (Primary Boot Loader) and MCP (Main Control Program). These subsystems cover all the IC dedicated software components listed in Section 3.2.1 of the *[ST]*.

Figure 2 below depicts the IC Dedicated Software block decomposition of the TOE:

- PBL subsystem is represented as the PBL block within the box labelled as "ROM SPU Firmware".
- MCP subsystem encompasses the blocks labelled as MCP, S.APP (Crypto app and Asym Crypto App) within the box labelled as "RAM - SPU software", plus the Mission ROM block within the "ROM SPU Firmware" box. Note, the OS boundary defined in Figure 2 is comprised of the MCP subsystem i.e. MCP, the system applications and Mission ROM.

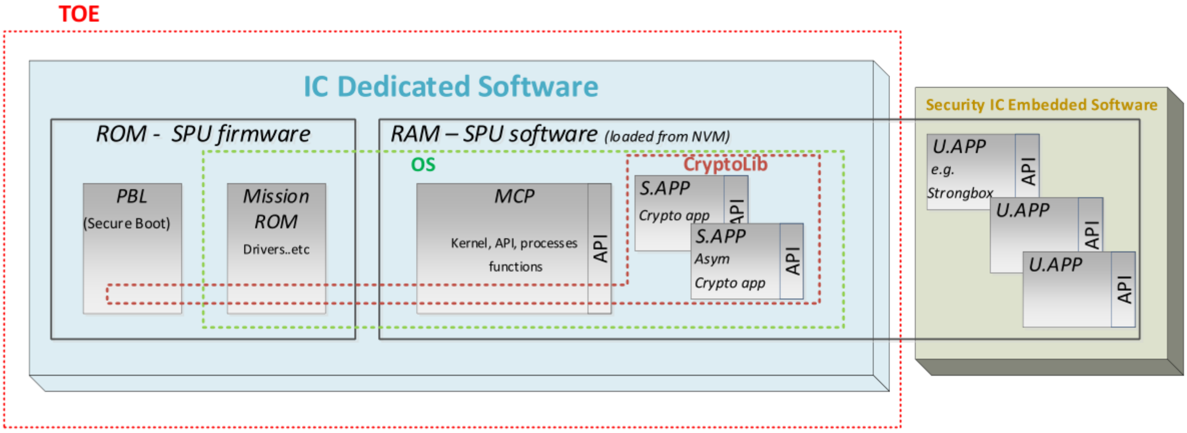

Figure 2: TOE software design decomposition

The PBL subsystem covers only the PBL part of the SPU firmware, whereas MCP subsystem includes all the SPU software part plus the Mission ROM part of the SPU firmware. The Mission ROM part of the SPU firmware is integrated with the PBL into a single ROM image during IC Development phase of the TOE lifecycle. However, in terms of TOE design breakdown, it is logically included in the MCP subsystem of the TOE. The CryptoLib boundary in Figure 2 corresponds with the Cryptographic Library, whose functionality is spread over the MCP and PBL design subsystems.

PBL subsystem contains a single module whereas MCP subsystem is further decomposed into modules with up to 3 levels of sub-modules. The high-level details of this decomposition are described below:

- PBL subsystem: It consists of the part of the SPU firmware stored in the ROM memory that is used for loading, decrypting, and authenticating the MCP and system application images stored in the non-TOE external memories present in the SOC.
  - The PBL subsystem is composed by a single module named Secure Boot.
- MCP subsystem: It is part of the SPU software comprising the Main Control Program itself (SPU Software including APIs and services for the system and user applications), the SPU system applications and the Mission ROM that includes drivers and low-level cryptography implementation. The Mission ROM is stored in the ROM memory whereas the rest of the MCP subsystem elements are stored in external SoC NVMs and then loaded into RAM for their execution. Below, the different modules of the MCP are listed. Those including logic in ROM are identified:
  - App: It consists of the SPU system applications in the user space. These include an Asymmetric Crypto App, providing asymmetric cryptographic services, and the Crypto App, providing symmetric cryptographic services.
  - App Wrappers: It consists of application's API implementations, usually wrappers of system calls.
  - Drivers: The driver layer of the MCP, containing drivers for clock, DMA, detection sensors, communication, NoC, Inter-process Communication (IPC) controller, interrupts, Power Management Integrated Circuit (PMIC), power management, timers and watchdogs. Parts of this logic are included in the Mission ROM firmware.
  - Kernel: Core of the SPU operating system, which includes sub-modules for handling crash dump, kernel entry points, ARM ETM tracing, external memory read and write to DDR, reaction in presence of fault detection, main kernel singleton object, handler of application manifests, miscellaneous functions to support kernel implementation, management of access rights to Memory Protection Unit (MPU), support for critical sections, interrupt controller, a handler for low-power mode, permission checker access to ROM/RAM to both user space and kernel space, process handler, ROM patch handler, ARM register handler, system parameters and system process handler, and timer interrupt handler. Parts of this logic are included in the Mission ROM firmware for low-level kernel operations.

- Middleware: Layer on the top of the drivers and Kernel that includes various sub-modules: a general-purpose application library, a crypto CMU module, a messaging sub-module handling IPC, and debug, error handling, heap and log management sub-blocks. Parts of this logic related to low-level crypto or messaging operations are included in the Mission ROM firmware.
- A shared Library providing functionality for countermeasures, runtime, cryptographic library wrappers, DES implementation, and ECC/RSA/RNG wrapping functionality over the CMU. Parts of its logic (low-level crypto or memory management operations) are included in the Mission ROM firmware.
- A system process sub-module, providing Non-Volatile Memory (NVM) system process (including ARI services) and SP-SC QFPROM system process main loops. Parts of this logic related to low-level application loading operations are included in the Mission ROM firmware.

2.5 Documentation

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

Identifier	**Version**
Secure Processor Unit (SPU) – Anti-replay Island (ARI) Overview for SM8350	80-PN145-16, Revision B
Qualcomm Secure Processing Unit Enablement for SM8350 Devices	80-PK177-4, Revision AD
Qualcomm Secure Processing Unit Enablement Guidelines for SM8350 Application Developers	80-PK177-5, Revision AB
SM8350 Secure Boot Enablement – User Guide	80-PK177-14, Revision AA
Secure Processor Unit SDK – API Reference	80-PV579-1, Revision AD
SMT Assembly Guidelines	SM80-P0982-1, Revision E
Qualcomm Trusted Execution Environment (TEE) Reference Manual	80-NH537-4, Revision M

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, subsystem and SFR-enforcing module level.

All parameter choices have been addressed at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. 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 hardware parts of the TOE, the developer performed three categories of testing: pre-silicon testing (simulation/emulation), post-silicon testing and production testing. These test categories are combined to achieve a good coverage and depth of testing, both on the design of the hardware parts of the TOE and on each of the manufactured ICs.

For the software parts of the TOE, the developer performed three categories of testing: simulation tests (including code coverage analysis), emulation and on-TOE testing. These categories were applied to the TOE to achieve a good coverage and depth of testing.

Amount of developer testing performed:

- The tests are performed on security mechanisms and on subsystem and module level with a total amount of several thousand test scenarios.
- As demonstrated by ATE_COV.2 the developer has tested all security mechanisms and TSFIs.
- As demonstrated by ATE_DPT.3 the developer has tested all the TSF subsystems and modules against the TOE design and against the security architecture description.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

All test results were as expected. No deviations were found.

2.6.2 Independent penetration testing

The methodical analysis performed was conducted along the following steps:

- When evaluating the evidence in the classes ASE, ADV and AGD the evaluator considers whether potential vulnerabilities can already be identified due to the TOE type and/or specified behaviour in such an early stage of the evaluation.
- For ADV_IMP a thorough implementation representation review is performed on the TOE focused on the Secure IC and the IC Dedicated Software. During this attack-oriented analysis, the protection of the TOE is analysed using the knowledge gained from all previous evaluation classes. This results in the identification of (additional) potential vulnerabilities. For this, analysis will be performed taking into account the attack methods in [JIL-AM] and applicable attack papers with rating according to [JIL-AAPS].
- All potential vulnerabilities are analysed using the knowledge gained from all evaluation classes and information from the public domain. A judgment was made on how to assure that these potential vulnerabilities are not exploitable. The potential vulnerabilities are addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 36 weeks. During that test campaign, 21,1% of the total time was spent on characterization tests, 5,6% on physical attacks, 12,2% on perturbation attacks, 61,1% on side-channel testing, and 0% on logical tests.

2.6.3 Test configuration

The testing was performed on earlier revisions of the TOE. The assurance gained from testing on earlier revisions has been assessed to be valid for the final TOE version, because the changes introduced were minimal and did not have an impact on the TSF. When Test OS is used, the JTAG interface for both the TOE and SOC was unlocked for the test devices for communication with TOE, ease of programming the devices with Test OS as well as to enable faster boot without involving the entire SOC bring up. Additionally, the SP-SC QFPROM configuration for the test devices allowed SOC to soft reset the TOE. Majority of the tests were executed using Test OS as custom test commands were required. The Test OS provided capabilities to disable some countermeasures for the evaluation purposes.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. The TOE supports a wider range of key sizes (see *[ST]*), including those with sufficient algorithmic security level to exceed 100 bits as required for high attack potential (AVA_VAN.5).

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities

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

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 2 site certificates and 2 Site Technical Audit Reuse reports.

In total 10 sites have been audited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support. The TOE can be identified as described in 80-PK177-4, Revision AD, as referenced in the *[ST]*.

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 *[COMP]* 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 Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SoC (Qualcomm® Snapdragon™ 888) with symmetric and asymmetric crypto support, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 “Documentation” contains necessary information about the usage of the TOE.

This TOE is critically dependent on the operational environment, namely the objective for the environment OE.Protect-Shared-Comp as defined in the *[ST]*, to provide countermeasures against specific attacks as described in section 2.3.1 of the user guidance 80-NH537-4 Rev.M as referenced in the ST.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength to satisfy the AVA_VAN.5 “high attack potential”. To be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The Qualcomm SPU250 Security Target, 80-NU430-5, Rev. AE, 26 November 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:

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
DES	Data Encryption Standard
DFA	Differential Fault Analysis
ECB	Electronic Code Book (a block-cipher mode of operation)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMA	Electromagnetic Analysis
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SPA/DPA	Simple/Differential Power Analysis
TOE	Target of Evaluation
TRNG	True Random Number Generator

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

[COMP] Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018

[ETR] Evaluation Technical Report for Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SOC with symmetric and asymmetric crypto support, Document ID 1930101-D3, Version 1.3, 26 November 2021

[ETRfC] ETR for composite evaluation Qualcomm Secure Processor Unit SPU250 (Version: 4.1) in SM8350 SOC with symmetric and asymmetric crypto support, Document ID 1930101-D4, Version 1.3, 26 November 2021

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution)

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019

[ST] Qualcomm SPU250 Security Target, 80-NU430-5, Rev. AE, 26 November 2021

[ST-lite] Qualcomm SPU250 Security Target Lite, 80-NU430-8, Rev. AD, 26 November 2021

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)