Certification Report

Qualcomm Secure Processor Unit SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and 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-2200044-01-CR**
Report version:	**1**
Project number:	NSCIB-**2200044-01**
Author(s):	**Hans-Gerd Albertsen**
Date:	**16 June 2023**
Number of pages:	**18**
Number of appendices:	**0**

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, TrustCB 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 TrustCB 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 TrustCB 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, TrustCB 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

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 SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and symmetric and asymmetric crypto support. The developer of the Qualcomm Secure Processor Unit SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and 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 an integrated Secure Element, composed by the subsystems Secure Processor Unit (SPU) and Trusted Management Engine (TME), which are integrated in the SoC within a stacked DDR package on SoC package (package form factor is non-TOE). It is designed as a tamperproof 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.

It is important to note that the involvement of the TME subsystem in the TOE is limited as a SFR-supporting component to support the SPU during the secure boot process. The TME subsystem participates in the secure boot of the entire platform and in particular, the only activities in the scope of the evaluation as SFR-supporting are the ones related to the boot of the SPU. The security features provided by TOE are limited to SPU hardware and firmware.

The TOE is comprised of a hardware layer, and IC Dedicated Software providing interfaces for application developers.

The TOE will allow for dedicated applications to execute on the operating system of the TOE to provide security services as listed above. Those applications are not part of the TOE, but the TOE operating system provides services to verify the integrity and authenticity of such applications using digital signatures.

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 communicates with the other components of the SoC either using shared memory or using shared Configuration and Status Registers (CSRs), interrupts, and power control messages.

The TOE has been evaluated by Riscure B.V. located in Delft, The Netherlands. The evaluation was completed on 16 June 2023 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 SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and 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 SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and 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).

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

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).

TrustCB 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.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Qualcomm Secure Processor Unit SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and 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	SPU260 hard macro embedded in SM8475 SoC	5.5
	TME hard macro embedded in SM8475 SoC	1.0.5
	Foundry ID embedded in SM8475 SoC	0
Firmware	SPU ROM code • PBL • Mission ROM	77100000
	TME CPU ROM code • TME PBL • TME Mission ROM	Linked to TME hard macro
	TME Sequencer ROM code • TME Sequencer Firmware	Linked to TME hard macro
Software	SPU Software image, which includes MCP and following system applications: • cryptoapp • asym_cryptoapp • nvm_sysproc	SPSS.A1.1.6.1-00032-PALIMA-1
	TME Sequencer Software image	Build release string ▪ 53 45 51 5F 46 57 5F 52 45 4C 45 41 53 45 5F 42 55 49 4C 44 5F 56 45 52 53 49 4F 4E 5F 53 54 52 49 4E 47 3D 72 39 (“SEQ_FW_RELEASE_BUILD_VERSION_STRING=r9” in ASCII)
	TME Core Software image	Build time string ▪ 4D 61 79 20 30 35 20 32 30 32 32 20 61 74 20 31 36 3A 30 32 3A 34 34 (“May 05 2022 at 16:02:44” in ASCII) Version string ▪ 73 73 67 2E 74 6D 65 66 77 2E 31 2E 30 2E 31 2D 30 30 32 39 39 2D 72 65 6C 65 61 73 65 (“ssg.tmefw.1.0.1-00299-release” in ASCII) Chipset string ▪ 57 61 69 70 69 6F (“Waipio” in ASCII)

SoC identifier

Item	Identifier
SM8475 SoC	A0080000

To ensure secure usage a set of guidance documents is provided, together with the Qualcomm Secure Processor Unit SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and 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 *[ST]* and are categorized as follows:

- Internal Security functions:
  - Access control to the various memories (OTP, RAM, ROM) and peripherals
  - Access control to keys managed in hardware through enforcement of key policy
  - Secure boot and secure loading of TOE software stored outside the TOE using the TOE root of trust (ROM code and TME subsystem)
  - Protection of User Data stored outside the TOE
  - Secure loading of user applications stored outside the TOE
  - Secure update mechanism of the TOE software or applications
  - Domain separation between applications executed by the TOE (for both user and system applications)
  - Anti-replay island and software freshness protection
- Cryptographic services (API):

  The TOE provides cryptographic services using the support of the Crypto Management Unit. Services provided through the API for user applications are as follows:

  - Generation of random numbers (used for key generation)
  - Secure key storage providing the possibility to have keys stored in the SP-CMU that are not readable by the SP-CPU. The SP-CPU can only request to perform cryptographic operations using those keys.
  - Secure key generation and zeroization
  - Symmetric encryption and decryption using the following:
    - AES with 128 bit and 256 bit keys
    - TDES with 112 bit and 168 bit keys
  - Hash functions: SHA-1, SHA-256, SHA-384, SHA-512
  - HMAC using keys up to 512 bit length and using SHA-1, SHA-256, SHA-384 or SHA-512
  - CMAC with AES using 128 bit and 256 bit keys
  - Asymmetric cryptographic operations:
    - RSA 1024 bit and 2048 bit
    - Elliptic curves cryptography with NIST P-192/224/256/384/521, Brainpool P-192/224/256/320/384/512 non-twisted (r1) and Curve25519 curves.
- Physical protection

  The TOE provides a number of functions and features that are designed to counter physical

attacks. Those include the following:

- Memory scrambling/memory encryption
- Side-channel analysis countermeasures
- Fault attacks sensors and countermeasures
- Memory/registers integrity checking

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 6.2 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.

2.4 Architectural Information

The TOE design is composed of four subsystems, two Hardware subsystems and two subsystems covering the IC Dedicated Software. Details are included in following sections.

Hardware subsystems

The hardware design of the TOE is decomposed into two different subsystems: a subsystem named HW, representing the SPU HW and a subsystem named TME_HW, representing the TME HW. HW subsystem (SPU) includes all the hardware components of the SPU, 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.

On the other hand, TME_HW subsystem includes all the hardware components of the TME, such as CPU, CPU ROM, CPU RAM, XPU-C, HW CSR, Sequencer, PRNG, Debug, HSDMA, Key Table, Sequencer ROM, Sequencer RAM, Fuse controller, Asymmetric and Symmetric Crypto, Clock controller and SCSR XPU4.

Figure 1 below provides details on the hardware subsystem structure.

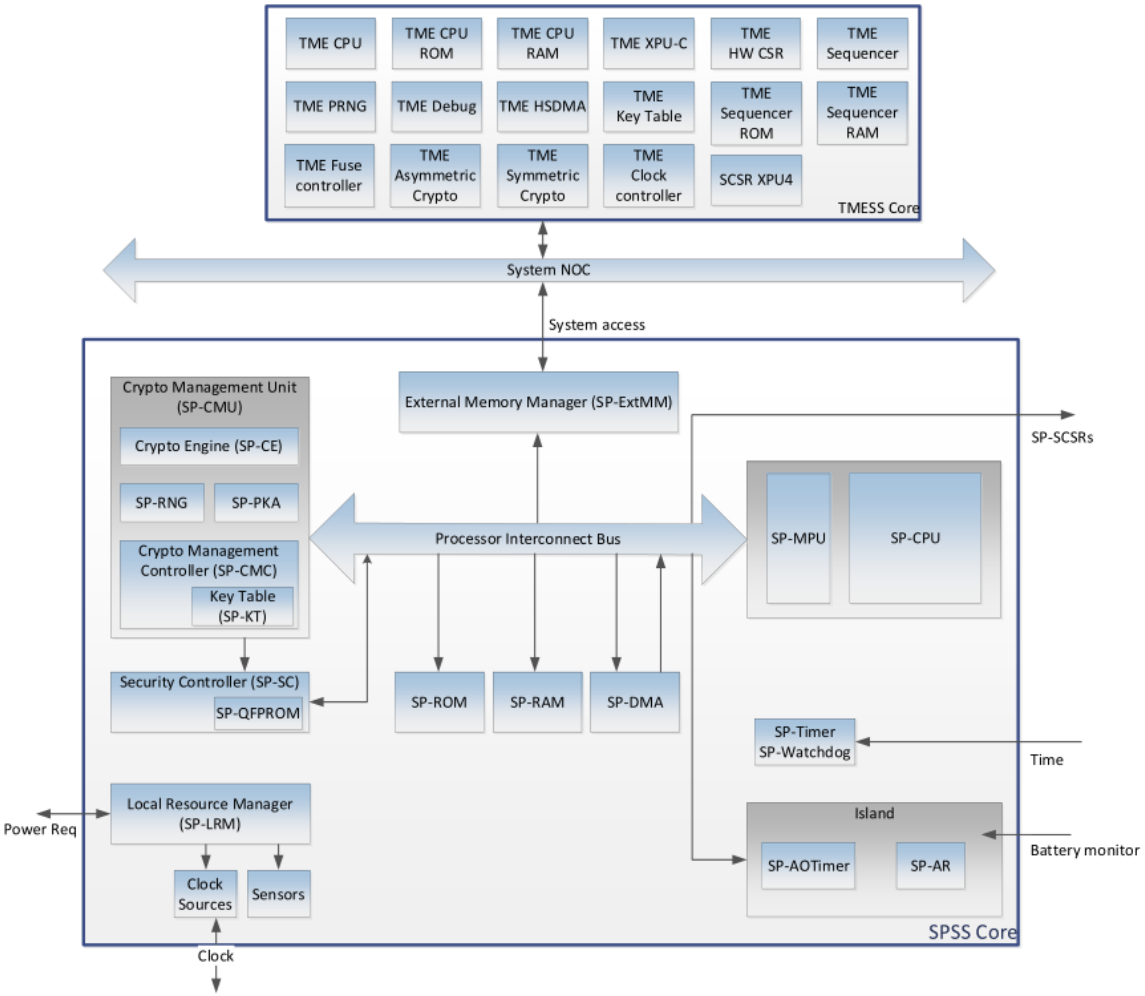

Figure 1: TOE hardware design decomposition

The TOE HW subsystem (SPU HW) 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 with an 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.

- 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.

The TME_HW subsystem is decomposed into various modules, and some of them are further decomposed into an additional level of sub-modules. The higher-level modules of the TME_HW subsystem are the following:

- CPU: Hardened CPU including a RISC-V Core, AXI master to SNoC with address remappers, CNoC Bridge as entry point to TME, ROM and RAM memories.
- Sequencer, controlling all the resources under TME hardware layer.
- Symmetric Crypto, performing symmetric cryptographic operations for the sequencer.
- Asymmetric Crypto, providing ECC and RSA based asymmetric cryptography services to TME CPU and SoC through the Sequencer.
- Fuse Controller, controlling the QFPROM OTP Memory of TME.
- Key Table that stores the keys used by the crypto engines on TME.
- HW CSR, register map used by the CPU or JTAG to execute commands on the sequencer.
- Clock Controller, controlling the clocks of the TME.
- Debug module, controlling TME debug functionalities.
- XPU-C, access control protection units.
- PRNG, Hardware/only random number generator.
- HSDMA, a high-speed Direct Memory Access unit.

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.

IC dedicated software subsystems

IC Dedicated Software comprises the SPU Firmware, SPU Software, TME Firmware and TME Software. The developer provides a logical design decomposition of the IC Dedicated Software into three subsystems: MCP (Main Control Program, representing SPU Software and part of SPU Firmware), PBL (Primary Boot Loader representing part of the SPU Firmware) and TME (representing the TME Software and TME Firmware). These subsystems cover all the IC Dedicated Software components listed in Section 2.1.

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

- PBL subsystem (covering part of SPU Firmware) is represented as the PBL block within the box labeled as "ROM SPU Firmware".
- MCP subsystem encompasses the blocks labelled as MCP, S.APP (Crypto app, Asym Crypto App and Nvm sysproc app) within the box labelled as "RAM - SPU software", plus the Mission ROM block within the "ROM SPU Firmware" box. Note, the SPU OS boundary defined in Figure 5.2 is comprised of the MCP subsystem i.e. MCP, the system applications and Mission ROM.

TME subsystem (covering TME Software and TME Firmware) encompasses the blocks labelled as "ROM – TME Firmware" and "RAM - TME Software".

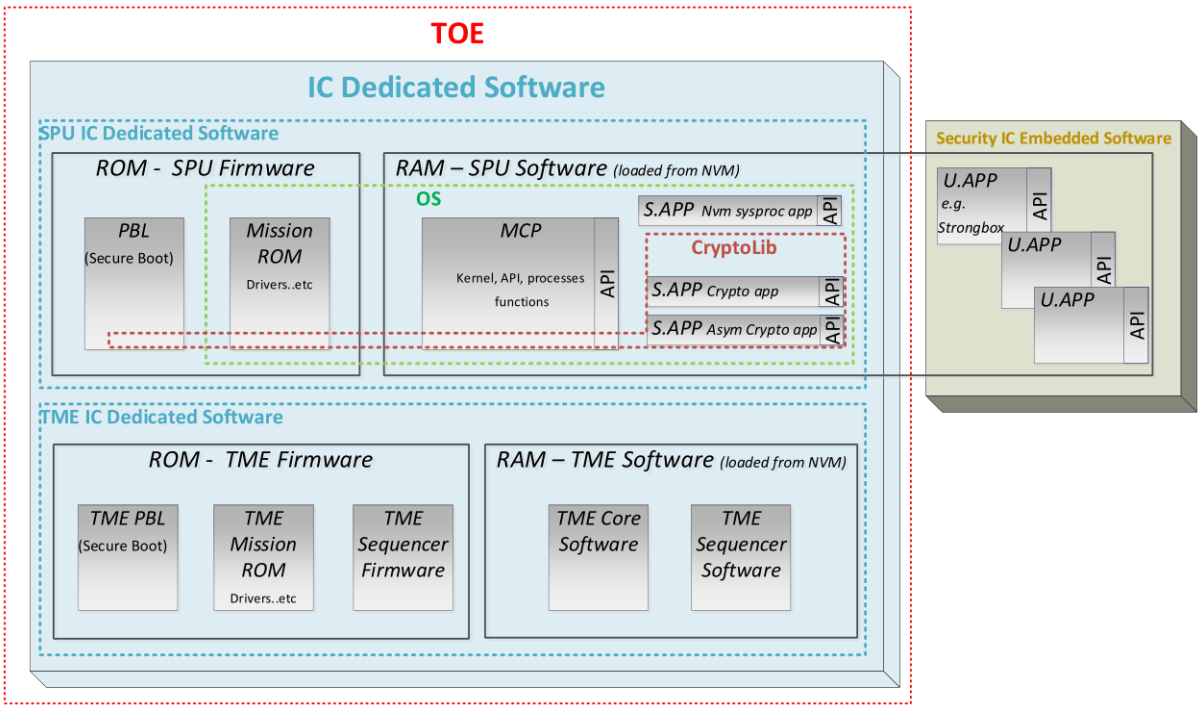

Figure 2: TOE software design decomposition

The PBL subsystem covers only the PBL part of the SPU firmware, whereas MCP subsystem includes all the SPU software part plus the SPU Mission ROM part of the SPU firmware. The SPU 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 SPU Mission ROM that includes drivers and low-level cryptography implementation. The SPU 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, the Crypto App, implementing symmetric cryptographic services, and NVM Proc app used for management of external NVM partitions.
    - App Wrappers: It consists of application's API implementations, usually wrappers of system calls.
    - Buses: It implements SPI and I2C protocols.
    - 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, MAC (Mandatory Access Control checking for system calls, system parameters and privileges), 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, including SP-SC QFPROM, system process main loops and lifecycle handler implementing the SPU lifecycle. Parts of this logic related to low-level application loading operations are included in the Mission ROM firmware.

TME subsystem comprises all the TME Software and TME firmware layers of TME. It is divided into various sub-modules, where most of them are divided further into a second level of sub-modules. The top-level modules of the TME subsystem are as follows:

- TME PBL module: it consists of the part of TME Firmware that resides in the TME CPU ROM memory. It is used for secure boot of the TME and performs authentication of the TME Core Software image. This module does not have any sub-modules.
- TME Sequencer FW: it consists of the part of TME Firmware that resides in the TME Sequencer ROM memory. It verifies the TME Sequencer Software in TME Sequencer RAM prior to the TME Sequencer Software is executed. This module is divided into an additional level of sub-modules that implement different services: provisioning, crypto primitives as trust level-0 Image Boot Service to be called from Level 1 (ROM), configuration shared register services, manager of TME Firmware lifecycle states, symmetric cryptography interfaces between TME firmware and hardware, fuse management service, clock controller, RNG FW layer, FIFO driver, HW initialization service, Asymmetric crypto services, debug services, key management services and access control functions.
- TME Sequencer SW: it consists of the part of the TME Software that runs on TME Sequencer RAM, and it manages the communication with registers and clocks. In terms of architecture, it is divided in the same sub-modules as TME Sequencer FW, since both modules share the same codebase. Some services of this sub-modular decomposition are designed in a way that the service behaves differently depending on whether it is executed in TME Sequencer ROM or RAM memory.
- TME Core SW: it consists of the part of the TME Software that runs on TME CPU RAM, and it also covers parts of the TME Firmware running on TME CPU ROM. Specifically, this module covers the TME MissionROM which is integrated with the TME PBL into a single ROM image that resides in TME CPU ROM. The main function of this module is supporting the secure boot of the SPU. It is divided in a number of sub-modules that implement different functionalities, such as: Qualcomm Mailbox Protocol implementation for IPC, secure Real-Time Operating System, Command handler managing I/O on the TME, CBOR implementing Concise Binary Object Representation protocol, SPU Service in charge of secure bring-up or tear down of the SPU, boot service in charge of start-up and boot of SoC, subsystem restart (not covering SPU restart), crash dump handler, secure boot service, debug service, Relay Message Buffer IPC, Access Control managing Soc-level resources and protection, Static access control function, key management service, TME lifecycle state manager, DMA engine services, Resource Power Management hardened service, Fuse management service, CPU configuration service,

CSR for ROM patching, secure boot image services for SoC IPs, cryptographic APIS, Peripheral Image loader and image verifier.

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 SM8450/SM8475	80-11140-16, Revision AC
Qualcomm® Secure Processing Unit Enablement for SM8450/SM8475 Devices – User Guide	80-PV345-150, Revision AG
SM8450/SM8475 Security Guidance for Secure Processing Unit Application Developers	80-PV345-152, Revision AE
SM8450/SM8475 Secure Boot Enablement	80-PV345-14, Revision AF
SM8450/SM8475 Secure Processor Unit SDK – API Reference	80-PV579-11, Revision AE
Qualcomm® Snapdragon™ Secure Processing Unit (SPU) Application Development User Guide	80-NU430-7, Revision AB
SMT Assembly Guidelines	SM80-P0982-1, Revision E

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 performed extensive testing on functional specification, subsystem, and SFR-enforcing module level.

All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively 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, as well as executing 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 considered whether potential vulnerabilities could 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 was performed on the TOE focused on the TOE hardware 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 resulted in the identification of (additional) potential vulnerabilities. The analysis was performed taking into account the attack methods in [JIL-AM] and applicable attack papers with rating according to [JIL-AAPS].

- All potential vulnerabilities were 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 were addressed by penetration testing, a guidance update or in other ways that are deemed appropriate.

The total test effort expended by the evaluators was 21 weeks. During that test campaign 61,9% of the total time was spent on characterization tests, 23,8% of the total time was spent on Perturbation attacks and 14,3% on side-channel testing.

Note: The TOE is considered as a delta of the TOE certified under NSCIB-CC-22-0436062. The evaluator used the developers Impact Analysis Report as leading input for the evaluation. Thereby, the test plan is not as comprehensive as for the TOE certified under NSCIB-CC-22-0436062 as some of the results from that evaluation are re-used supported with verification testing.

2.6.3 Test configuration

The TOE hardware and firmware versions for all executed tests were the same as stated in section 2.1 above. The 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. When Test OS was used, the JTAG interface for both the SPU and SoC was unlocked for the test devices for communication with SPU, ease of programming the devices with Test OS as well as to enable faster boot without involving the entire SoC bring up.

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 thirteen (13) Site Technical Audit Report{s}.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Qualcomm Secure Processor Unit SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and symmetric and asymmetric crypto support. The TOE can be identified as described in 80-PV345-150, Revision AG, 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, and Site Technical Audit Reports for the sites *[STAR]* [2]. 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 SPU260 (Version: 5.5) in SM8475 SoC (Qualcomm® Snapdragon™ 8+ Gen1) with TME (Version 1.0.5) and 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]*.

The Security Target claims conformance to the Protection Profile *[PP]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" 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 concerning 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 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).

[2] The Site Technical Audit Report contains information necessary to an evaluation lab and certification body for the reuse of the site audit report in a TOE evaluation.

3 Security Target

The Qualcomm SPU260 (v5.5) Security Target, 80-NU430-15, Rev. AC, 25 May 2023 *[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
CMAC	Cipher-based MAC
CNoC	Config Network on Chip
CSR	Configuration and Status Registers
DES	Data Encryption Standard
DDR	Double Data Rate
HMAC	Hash-based MAC
HSDMA	High Speed Direct Memory Access
IC	Integrated Circuit
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
MAC	Message Authentication Code
MCP	Main Control Program
NSCIB	Netherlands Scheme for Certification in the area of IT Security
PP	Protection Profile
PRNG	Pseudo RNG
QFPROM	Qualcomm Fuse-Programmable Read-Only Memory
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman Algorithm
SHA	Secure Hash Algorithm
SCSR	Shared Configuration and Status Registers
SNoC	System Network on Chip
SoC	System on Chip
SP-CMU	Secure Crypto Management Unit
SP-CPU	Secure Central Processing Unit
SPU	Secure Processor Unit
TDES	Triple DES
TME	Trusted Management Engine
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 SPU260 (Version: 5.5) in SM8475 SoC with TME (Version: 1.0.5) and symmetric and asymmetric crypto support, Document ID 2130091-D3, V1.1, 13 June 2023
[ETRfC]	ETR for composite evaluation Qualcomm Secure Processor Unit SPU260 (Version: 5.5) in SM8475 SoC with TME (Version: 1.0.5) and symmetric and asymmetric crypto support, Document ID 2130091-D4, V1.1, 13 June 2023
[JIL-AAPS]	JIL Application of Attack Potential to Smartcards, Version 3.2, November 2022
[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 2.6, 02 August 2022
[PP]	Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014
[ST]	Qualcomm SPU260 (v5.5) Security Target, 80-NU430-15, Rev. AC, 25 May 2023
[ST-lite]	Qualcomm SPU260 (v5.5) Security Target Lite, 80-NU430-16, Rev. AA, 02 May 2023
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006

(This is the end of this report.)