Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1045-V2-2023

for

Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP version spss.a1.1.2_00100

from

Qualcomm Technologies Inc.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1045-V2-2023 (*)

Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP
version spss.a1.1.2_00100

from	Qualcomm Technologies Inc.
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5 and ALC_DVS.2

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2

Bonn, 3 March 2023

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Sandro Amendola L.S.
Head of Division

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern und für Heimat (Federal Ministry of the Interior and Community)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

[4] Proclamation of the Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 components.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP, version spss.a1.1.2_00100 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1045-2019. Specific results from the evaluation process BSI-DSZ-CC-1045-2019 were re-used.

The evaluation of the product Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP, version spss.a1.1.2_00100 was conducted by Deutsche Telekom Security GmbH and atsec information security GmbH. The evaluation was completed on 22 February 2023. Deutsche Telekom Security GmbH and atsec information security GmbH are evaluation facilities (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Qualcomm Technologies Inc..

The product was developed by: Qualcomm Technologies Inc..

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 3 March 2023 is valid until 2 March 2028. Validity can be renewed by re-certification.

[5] Information Technology Security Evaluation Facility

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,
2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP, version spss.a1.1.2_00100 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Qualcomm Technologies Inc.
5775 Morehouse drive
San Diego, CA 92121
USA

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is the “Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP version spss.a1.1.2_00100”. The TOEs hardware and firmware are embedded in the SDM855 host SoC combined with a DDR in a PoP (Package-on-Package) configuration and its corresponding Software.

The hardware is a hard macro (sub-unit of a System-on-Chip which is already synthesized, placed and routed, delivered as GDS file) and the special packaging. The TOE is integrated into the SDM855 SoC by the SoC integrator (Qualcomm).

The firmware and software comprise the operating system of the secure processing unit and the software API providing symmetric and asymmetric cryptographic services to SPU applications. The SPU applications can be developed by the SPU application developer using the software API.

The TOE can be used for multiple applications that require a high level of security. Examples are as follows: User authentication and password storage, Content protection, Payment, Subscriber Identity Module (SIM), Storage and management of digital identities, secure key storage, Root of trust, Storage of sensitive user data (e.g., health care records).

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by AVA_VAN.5 and ALC_DVS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [9], chapter 8. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
Cryptographic services and random number generation	Random number generation, AES coprocessor, Hashing, Authentication, Key derivation function, Key protection, TDES, Asymmetric crypto
Secure boot and secure update	Secure boot, Secure software update
Application manager	User data and TSF data of different applications is only accessible by the associated application.
Domain separation between applications executed by the TOE	Dedicated control for the access to external memory as well as for the access to internal memories and resources that can be configured in privileged mode.
Physical protection	Protection mechanisms against non-invasive, semi-invasive, and invasive physical attacks.
Access control and management (hardware)	Control memory areas shared with other components of the SoC, control access to keys

TOE Security Functionality	Addressed issue
	and the key table, control use of hardware support for cryptographic operations and random number generation, control access to the SP-RAM by software on the SP-CPU
Access control and management (operating system)	Cryptographic protection of persistent data stored outside the TOE, Cryptographic protection of transient data and code stored outside the TOE, Reallocation of shared resources
Logical protection	SP-ROM, SP-RAM
Production data and OTP handling	Data for the identification of the TOE and the associated initialization and pre-personalization data is stored in the SP-QFPROM.
Lifecycle control	Lifecycle control based on a combination of access control to TOE functionality and the coding of the lifecycle phase in the SP-QFPROM.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 9.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 5.1 . Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 5.2 to 5.4.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP, version spss.a1.1.2_00100

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	Hard macro	SPU230 hard macro (GDS) containing hardware design and ROM	3.1	GDS
2	Hardware	SoC embedding the SPU hard macro SDM855	V2.2	bare die

No	Type	Identifier	Release	Form of Delivery
3	Hardware	Party packaged SoC	PX90-PC761-5	Packaged bare die without DDR[7]
4	Firmware	ROM image - Secure boot loader (PBL) and platform API code (MissionROM)	MissionROM: ROM_V2_BINARIES_0 PBL: SDM855_SPSS_PBL_V2	Included in SPU hard macro ROM
5	Software	MCP image	spss.a1.1.2_00100	Software image encrypted and signed
6	Software	System application - cryptoapp image	spss.a1.1.2_00100	Software image encrypted and signed
7	Software	System application - asym_cryptoapp image	spss.a1.1.2_00100	Software image encrypted and signed
8	Document	Qualcomm SPU Core – Hana API	4.6	PDF [11]
9	Document	80-PD867-16_ Secure Processor Unit ARI	B	PDF [12]
10	Document	80-PF777-83_ SPU_Enablement_UG	AC	PDF [13]

Table 2: Deliverables of the TOE

2.1. Overview of delivery procedures

The TOE hardware and firmware (ROM) including the personalization data (in SP-QFPROM) will be delivered in the form of a partly packaged SoC to the device manufacturers. The device manufacturer integrates the SoC into his devices.

The integration include the step of adding a DDR package on top of the partly packaged SoC. This is called Package-on-Package (PoP). The DDR is required to operate the TOE.

In addition, the device manufacturers will receive the TOE software (MCP image and System Applications) as part of an overall Qualcomm SW package for the SoC. Qualcomm provides customers access to the Agile system that can be used to download the SW package.

The TOE software will be loaded by the device manufacturer in the non-volatile memory (e.g. flash memory) implemented on the devices.

Also, the guidance documents listed in the table “TOE Deliverables”, can be downloaded from the data based provided in Agile.

Delivery protection for all TOE components is covered by ALC_DEL and ALC_DVS.

2.2. Identification of the TOE by the user

The developer provided a health API that can be used to read out the configuration of the device and determine the hardware identifier. An additional verification step is the test of the device with the encrypted and signed software provided by Qualcomm. The integrator has a procedure (refer to [13], section 11.1) to verify the integrity of the software image

[7] The final TOE is the partly packaged SoC delivered to the OEM combined with a packaged DDR (according to the requirements of the User Guidance 80-PF777-83) resulting in a Package on Package (PoP) form factor.

using SHA-256. Since the software is encrypted, the software can only be executed after a successful decryption inside the secure processing unit.

The SoC related guidance documents can be downloaded by the customers using the Agile system. Agile is only accessible to registered user and provides a transport protection of the data exchanged with the Agile data base.

The description of the Software API is provided to customers separately in encrypted form.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

Protection against leakage of information, against physical probing, against malfunctions, against physical manipulations and against abuse of functionality. Hence the TOE maintain

- the integrity and the confidentiality of data stored in the memories and the key table of the TOE,
- the integrity, the correct operation and the confidentiality of security functionalities (security mechanisms and associated functions) provided by the TOE, and
- the integrity, authenticity, confidentiality and relay-protection of data stored outside the TOE.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

Regarding the operational environment of the TOE, the security objectives OE.Resp-Appl (Treatment of User Data of the Composite TOE), and OE.Process-Sec-IC (Protection during composite product manufacturing) are relevant for the user in context of secure installation of the TOE and the secure preparation of the operational environment. All objectives are properly covered by user guidance.

Details can be found in the Security Target [6] and [9], chapter 6.2.

Details on OE.Process-Sec-IC are provided with the guidance for configuration before the delivery to the end user in [13]. In addition, requirements regarding the device where the Qualcomm Secure Processing Unit SPU230 with MCP version spss.a1.1.2_00100 is integrated, is provide in [12].

Details on OE.Resp-Appl are provided in [11].

5. Architectural Information

The TOE comprises the independent secure processing unit (subsystem) integrated in a System-on-Chip (SoC). The secure processing unit serves as an independent Root of Trust within the SoC. It does not rely on any external entity for any security enforcement, allowing it to be evaluated as a separate entity. It has its own ROM code for secure boot operations.

The hard macro consists of

- Secure Central Processing Unit, which executes the main code of the TOE
- RAM and ROM (including the Primary Boot Loader image)
- One-Time Programmable memory for life cycle management and to store initialization and pre-personalization data
- Cryptographic Management Unit, which includes the random number generator, the coprocessor for AES and SHA and holds a Key Table
- Local Resource Manager, which provides the interface to the clock, the reset line, and the interface to the sensors (voltage, temperature, logic fault, etc.)
- SP-Timer and SP-Watchdog, used to provide timer functionality for the TOE independent from the remaining SoC
- The External Memory Manager providing read/write capabilities to TOE external memory
- Always-on Island containing the anti-replay mechanism.

The software part of the TOE comprises Firmware, Operating Systems and Applications

- Firmware controls the secure boot process and contains drivers that are used in Operational Mode by the loaded software.
- The Operating System manages the access to the services provided by the TOE, implements software countermeasures and controls the applications.

The Operating System and System applications provide the following services to applications:

- Cryptographic services (AES, Hashing and message authentication codes, random number and generation of symmetric keys and asymmetric keys for elliptic curve algorithms)
- Storage for User data in the external non-volatile memory. User data is exported encrypted, authenticated and protected against replay. The TOE maintains a unique key for each application that stores User data in the external memory.
- Communication services with other entities of the SoC (e.g. Modem sub-system, HLOS or Trusted Execution Environment).
- Application loading services

The Qualcomm Secure Processing Unit SPU230 with MCP version spss.a1.1.2_00100 is the assembled device as Package-on-Package. One package contains the SoC with the Secure Processing Unit and the other package contains the DDR. The DDR is also used to swap code and User data during the operation. Also data stored in RAM is protected using encrypted, authentication mechanism and protected against replay.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

7.1. Developer's Test according to ATE_FUN

The tests performed by the developer cover the hard macro of the secure processing unit as well as the software that is part of the TOE. The testing is performed in different steps.

The silicon of the hard macro was tested separately using common test approaches for silicon. These tests comprise:

- Design verification using simulations based on tools provided with the development environment and using FPGA based hardware emulation.
- Characterization tests of the secure processing unit were part of the overall characterization tests for the SoC. The test capabilities and the test functionality implemented in the secure processing unit support the verification of the different sensors for frequency, voltage and temperature and other features that may depend on the operating conditions. These tests are performed with several samples for each test.
- Verification tests include the evaluation of security mechanisms implemented in the hard macro. These tests were performed using samples in test mode, debug mode and operational mode. Specific test setups are used depending on the configuration of the device.
- Production tests of the secure processing unit are a dedicated part of the overall production test for the SoC. Testing of the hard macro is implemented as combination of scan testing and functional tests. All functional security mechanisms are covered by these tests. The last step of the production tests includes the initialization and pre-personalization that was also verified.

The developer testing approach for software is mainly based on the use of automated test cases. These test cases are deployed onto the TOE and executed. The test applications are standalone and have no mutual dependencies. Test applications may have one or more test cases implemented. Each test case contains the expected test result. The test cases perform a verification step of the observed behaviour with the expected results. If the generated test results matches with the expected test results, the test cases return a pass verdict. Other-wise a fail verdict is returned. In addition specific manual tests were applied to verify specific security functionality of the hardware platform.

The developer’s testing demonstrates that the TSFs behave as specified.

7.2. Evaluator Tests – Independent Testing according to ATE_IND

Two different test configurations were delivered and used for testing:

- The hardware platform in debug mode with specific test framework and specific test software. This setup was used to test specific components of the secure processing unit beyond the capabilities provided in the operational mode.
- The final TOE comprising the secure processing unit with firmware and the software package. Together with a dedicated test application the evaluators were able to test the API provided by the TOE.

Most of the independent evaluator tests were performed in the evaluation lab. This comprises the tests as required by AIS 31, [4] for the random number generator. Some tests were executed on the FPGA implementation of the secure processing unit using test

software developed by the evaluator. In addition, tests of the developer were reproduced and additional tests were implemented to supplement the developer tests.

The independent evaluator tests confirm that the TOE provides the specified functionality and that the TSF behave as specified. The configuration of the hard macro with firmware and software as specified in the Security Target was considered during the tests.

7.3. Penetration Testing according to AVA_VAN

Penetration testing was partially performed using the developer's environment for testing and failure analysis. Side-channel, fault injection and parts of the sample preparation were performed in the lab of the evaluation facility.

For several tests the evaluators use specially prepared devices in debug mode to speed up testing, enable the verification of specific security mechanisms, support best case scenarios from the attacks point of view and anticipate successful complex preparation steps required by an attacker.

Additional penetration tests were performed using the final TOE configuration with specially prepared samples. The performed tests confirm the effective combination of countermeasures implemented in the hardware as well as in the firmware and software. Experience gained during the testing with samples in debug mode were used for this verification on the final TOE.

Systematic search for potential vulnerabilities and attacks according to the guidance provided in AIS 26, [4] have been conducted. In addition, indications for potential vulnerabilities noted during the evaluation of the hardware and software design were assessed. Potential attacks that could not be excluded based on the analysis form the basis for devised penetration tests.

The evaluator did not identify vulnerabilities that are exploitable in the intended environment for the TOE with high attack potential. Therefore the TOE is resistant to attackers with "high" attack potential in the intended environment of the TOE. This comprises all the usage of the software API and security functionality described in the Security Target [6].

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

There is only one evaluated configuration of the TOE. This configuration returns the following hardware version information.

Target ID:	SM8150xx
Hardware version:	02.xx
HW_REVISION_NUMBER.VERSION_ID:	x
Serial number:	individual
CHIP ID:	0x404
SP_CORE_HW_REVISION	
MAJOR:	0x3
MINOR:	0x1

The values were read from the hardware registers for identification.

The hard macro of the secure processing unit and the associated configuration are determined by the last row: SP_Core_HW-Revision 3.1 (MAJOR: 3, MINOR: 1). The “x” in the rows in the table above belong to the remaining part of the SoC and may change.

8.1. Precise description of the evaluated configuration of the TOE

The Qualcomm Secure Processing Unit SPU230 with MCP version spss.a1.1.2_00100 is trimmed and configured before the delivery. Only one configuration with respect to the Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP version spss.a1.1.2_00100 is delivered. The device manufacturer needs to finalise the configuration in the following way as outlined in [13], chapter 4:

The device manufacturer must configure the “Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP version spss.a1.1.2_00100” with

- SPU enabled and
- SPU anti-replay configuration active.

The enabling or disabling of the self-test as required for the FIPS compliance does not have an impact on the security of the TOE.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

- *The Application of CC to Integrated Circuits*
- *Application of Attack Potential to Smartcards*
- *Guidance, Smartcard Evaluation*

(see [4], AIS 25, AIS 26, AIS 37).

For RNG assessment the scheme interpretations AIS 31 was used (see [4]).

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure. It could be provided by the ITSEF and submitted to the certification body for approval subsequently.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components AVA_VAN.5 and ALC_DVS.2 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1045-2019, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the extended cryptographic services of the TOE.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014 [8]
- for the Functionality: PP conformant plus product specific extensions
- Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5 and ALC_DVS.2

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
1	Image Authenticity and Integrity	RSA-signature verification with SHA-256 and PKCS#1 1.5 padding	FIPS 186-4 FIPS 180-4 RFC3447	2048	Security Level >= 100 Bits
2	Image Confidentiality	AES-CBC	FIPS 197 NIST SP800-38A	128	Yes
3	User and TOE data while in NVM Confidentiality	AES-CBC	FIPS 197 NIST SP800-38A	256	Yes
4	User and TOE data while in NVM Integrity and Authenticity	SHA-256 tree and AES in CMAC mode	FIPS-180-4 FIPS 197 NIST SP800-38B Hash tree specifics provided in developer document	256	Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
5	User and TOE data while in external DDR Confidentiality	AES-CBC	FIPS 197 NIST SP800-38A	256	Yes
6	User and TOE data while in external DDR Integrity and Authenticity	SHA-256	FIPS 180-4	256	Yes
7	API	TDES (ECB, CBC)	FIPS46-3 SP800-38A	168	No
8	API	AES (ECB, CBC, CTR, CMAC, CCM)	FIPS 197 NIST SP800-38A NIST SP800-38B NIST SP800-38C NIST SP800-38E	128, 256	Yes
9	API	SHA1 SHA-256 SHA-384 SHA-512	FIPS 180-4	none	No Yes Yes Yes
10	API	RNG	PTG.3 According to AIS-31 NIST SP800-90A	none	N/A
11	API	HMAC-SHA1 HMAC-SHA256 HMAC-SHA-384 HMAC-SHA-512	FIPS198-1	256 (SHA-1, SHA-256) 512 (SHA-384, SHA-512)	No Yes Yes Yes
12	API	Generate random symmetric key	NIST SP800-90A	256	Yes
13	API	Key Derivation Function in Counter Mode based on HMAC SHA-256	NIST SP800-108 FIPS 198-1 FIPS 180-4	256, 512	Yes
14	API	RSA signature/verify with SHA-1, SHA-256, SHA-384, SHA-512 and RSASSA-PSS and PKCS#1 v1.5 padding schemes	FIPS 186-4 FIPS 180-4 RFC3447	1024, 2048	RSA-1024: No RSA-2048: Security-Level >= 100 Bits SHA1: No
15	API	RSA encryption / decryption with RSAES-OAEP and PKCS#1 v1.5 padding schemes	FIPS186-4 RFC3447	1024, 2048	RSA-1024: No RSA-2048: Security-Level >= 100 Bits
16	API	ECDSA Cryptographic key generation Signature Generation / Verification	FIPS186-4 Appendix B.4.2	ECC key lengths corresponding to following ECC parameters: NIST P-192, NIST P-224, NIST P-256,	 No No Yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 120 Bits
				NIST P-384, NIST P-521	Yes Yes
17	API	ECDH Cryptographic key generation Shared secret generation	SP800-56A revision 2 section 5.6.1.2 SP800-56A revision 2 section 5.7.1.2 FIPS 186-4 Appendix D.1.2	ECC key lengths corresponding to following ECC parameters: NIST P-192, NIST P-224, NIST P-256, NIST P-384, NIST P-521	 No No Yes Yes Yes

Table 3: TOE cryptographic functionality

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

Some security measures are partly implemented in this certified TOE, but require additional configuration or control or measures to be implemented by a product layer on top, e.g. the Embedded Software using the TOE. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the developer of the product layer on top on how to securely use this certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE. In the course of the evaluation of the composite product or system it must be examined if the required measures have been correctly and effectively implemented by the product layer on top. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in a document "ETR for composite evaluation".

At the point in time when evaluation and certification results are reused there might be an update of the document "ETR for composite evaluation" available. Therefore, the certified products list on the BSI website has to be checked for latest information on reassessments, recertifications or maintenance result available for the product.

11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
ARI	Anti-Replay Island
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DDR	Dobble Data Rate RAM
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FPGA	Field Programmable Gate Array
GDS	Graphic Design System
HW	Hardware
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MCP	Main control program
PoP	Package-on-Package
PP	Protection Profile
SAR	Security Assurance Requirement
SoC	System-on-Chip
SFP	Security Function Policy

SFR	Security Functional Requirement
SIM	Subscriber Identity Module
SPL	Secure boot loader
SP-RAM	SPU-RAM
SP-ROM	SPU-ROM
SP-CPU	SPU-CPU
SP-QFPROM	QFPROM
SPU	Secure Processing Unit
ST	Security Target
SW	Software
TDES	Tripple DES
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen)
https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8]
https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1045-V2-2023, Revision J, Date: 14.01.2022, Qualcomm SPU230 Core Security Target, Qualcomm Technologies, Inc., (confidential document)

[7] Evaluation Technical Report, Version 2.1, Date: 26.01.2023, Evaluation Technical Report - Summary for Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP version spss.a1.1.2_00100, Deutsche Telekom Security GmbH (confidential document)

[8] Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014

[9] Security Target BSI-DSZ-CC-1045-V2-2023, Revision H, Date: 14.01.2022, Qualcomm Secure Processing Unit SPU230 Core Security Target Lite, Qualcomm Technologies, Inc., (sanitised public document)

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 9, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 38, Version 2, Reuse of evaluation results

[10] Impact Analysis Report, Re-evaluation Secure Processing Unit SPU230, MCU SW Update: CM081 to CM100, Qualcomm Technologies, Inc., Revision 0.4, February 22, 2022

[11] Guidance documentation for the TOE: Qualcomm SPU Core, Hana Application Programming Interface API, Qualcomm Technologies Inc., Rev. 4.6, August 26th, 2020 (confidential document)

[12] Guidance documentation for the TOE: Secure Processor Unit (SPU) Anti-Replay Island (ARI), Overview for SM8150, Qualcomm Technologies Inc., Revision B, November, 2018 (confidential document)

[13] Guidance documentation for the TOE: Qualcomm Secure Processing Unit, Enablement, 80-PF777-965 AC, Qualcomm Technologies Inc., Rev. AC, May 6th, 2021 (confidential document)

[14] Configuration list for the TOE: Configuration List user guidance, TOE_user_guidance_config_list v13.pdf, 09th December 2021 (confidential document)

[15] Configuration list for the TOE: Configuration List hardware spec, TOE_HW_spec_config_list-4.0.xlsx, 04th April 2019 (confidential document)

[16] Configuration list for the TOE: Configuration List for the hardware platform, Qualcomm Technologies, Inc., version 3,1; 11th April 2019 (SPU_3_1_config_list.txt (confidential document)

[17] Configuration list for the TOE: Configuration list including the functional and verification tests of the hardware plat-form: TOE_HW_test_config_list.txt (confidential document)

[18] Configuration list for the TOE: pbl_v2_config_list.txt, 22.03.2019 (confidential document)

[19] Configuration list for the TOE: rom_v2_binaries.txt, 23.10.2018 (confidential document)

[20] Configuration list for the TOE: Configuration list of the documentation for the hardware development process TOE_SW_HW_process_config_list-10.1.pdf (confidential document)

[21] Configuration list for the TOE: Configuration list software specifications: TOE_SW_Docs_config_list.txt (confidential document)

[22] Configuration list for the TOE: Configuration list functional and verification tests of software: TOE_SW_Test_config_list_CC2_PHASE2.txt(confidential document)

[23] Configuration list for the TOE: MCP Software configuration list: config_list_spu_100.txt (confidential document)

[24] Configuration list for the TOE: Configuration list of the documentation for the software development process: ALC_CMC_Doc_config_list-5.2.pdf (confidential document)

[25] Configuration list for the TOE: Site Security Documentation Configuration List: Secproc_config_list.txt (confidential document)

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1045-V2-2023

Evaluation results regarding development and production environment

The IT product Qualcomm Secure Processing Unit SPU230 in SDM855 SoC with MCP, version spss.a1.1.2_00100 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5, and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 3 March 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

are fulfilled for the development and production sites of the TOE listed below:

Company	Life Cycle	Location	Service
Qualcomm	Phase 1, 2, 5 (HW and SW)	Pacific Center Blvd Ste 100 92121 San Diego USA	Hardware and software development, integration into the SoC, test program development and integration as well as device bring-up
Qualcomm	Phase 1	Omega Building, 4th Floor, Tirat Hacarmel, Haifa, Israel	Software development
Qualcomm	Support	IT Workspace Bangalore, room E-050J, India	IT administration of Sparrow and network
Qualcomm	Phase 5	Qualcomm Singapore 51 Alps Ave, #03-04/07, Singapore 498783	Shipping
TSMC BSI-DSZ-CC-S-0217-2022	Phase 3a, 3b, 3c	TSMC Fab15A, Fab15B, CP03 Taichung, Taiwan, R.O.C.	Mask production, Wafer production, Wafer Test
TSMC DSZ-CC-S-0218-2022	Phase 3a, 3b, 3c	Fab 2/5, Fab 3, Fab 7, Fab 8 and Fab 12P4/P5/P6/P7 Hsinchu, Taiwan, R.O.C.	Support of TSMC Fab15A, Fab15B
Amkor BSI-DSZ-CC-S-0170-2020	Phase 3c	1F, No. 1, Kao-Ping Sec, Chung-Feng Road, Lungtan Township, Taoyuan County 325, Taiwan, R.O.C.	Bumping and probe test
SPIL BSI-DSZ-	Phase 3c	SPIL ZK factory, No 19	Bumping and probe test

CC-S-0197-2022		Keya Road, Daya District, Taichung, Taiwan, R.O.C.	
Amkor	Phase 4	Site K4 Gwangju 100, Amkor-ro, Buk-gu Gwangju 61006 Korea	Assembly
Amkor	Phase 4/5	Site K5 Songdo 150, Songdo-mirae-ro Yeonsu-gu, In-cheon 21991 Korea	Only IT support for K3 and K4
Amkor	Phase 5	Site K3 Bupyeong 110, Anaji-ro, Gyeyang-gu In-cheon 21107 Korea	Final test and provisioning
Amkor	Phase 4	921-3, Himega-wara, Myoko-shi, Niigata, 944-8588 Japan	Assembly

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.

Note: End of report