Certification Report

Qualcomm Secure Processor Unit SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support

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

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

Report number:	**NSCIB-CC-2300004-02-CR**
Report version:	**1**
Project number:	NSCIB-**2300004-02**
Author(s):	**Jordi Mujal**
Date:	**16 April 2024**
Number of pages:	**13**
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 SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support. The developer of the Qualcomm Secure Processor Unit SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support is Qualcomm Technologies, Inc. located in San Diego, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is an integrated Secure Element, composed by the subsystem called Secure Processor Unit (SPU), which is integrated in the SoC within a stacked DDR package on SoC package (package form factor is non-TOE). It is designed as a tamper resistant device providing secure storage and a secure execution environment for processing of sensitive data and for performing cryptographic operations using protected keys stored in its secure storage. Secure Elements can be used for multiple application areas that require a high level of security.

The TOE was evaluated initially by Riscure B.V. located in Delft, The Netherlands and was certified on 10 November 2023. The re-evaluation of the TOE has also been conducted by Riscure B.V. and was completed on 16 April 2024 with the approval of the ETR. The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a “recertification with major changes”.

The major changes are:

- Change of security assurance level from EAL4+ to EAL5+

The security evaluation reused the evaluation results of previously performed evaluations. A full, up-to-date vulnerability analysis has been made.

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 SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Qualcomm Secure Processor Unit SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

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.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Qualcomm Secure Processor Unit SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support from Qualcomm Technologies, Inc. located in San Diego, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SPU hard macro embedded in SM8650 SoC[2]	7.0
	Foundry ID embedded in SM8650 SoC	0
Firmware	SPU ROM code • PBL • Mission ROM	77100100
Software	SPU MCP image, which includes MCP and following system applications: • cryptoapp • asym_cryptoapp • nvm_sysproc	SPSS.A1.1.9-00052-LANAI-1

To ensure secure usage a set of guidance documents is provided, together with the Qualcomm Secure Processor Unit SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support. For details, see section 2.5 “Documentation” of this report.

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

2.2 Security Policy

The TOE maintains:

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

This is ensured by the construction of the TOE and its security functionality. The major security features of the TOE are described in Section 2.3 of *[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)
    - 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)

[2] TOE is integrated into SM8650 SoC with identifier A00C0000.

- Anti-replay island and software freshness protection

- Cryptographic services (API):
  - 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.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

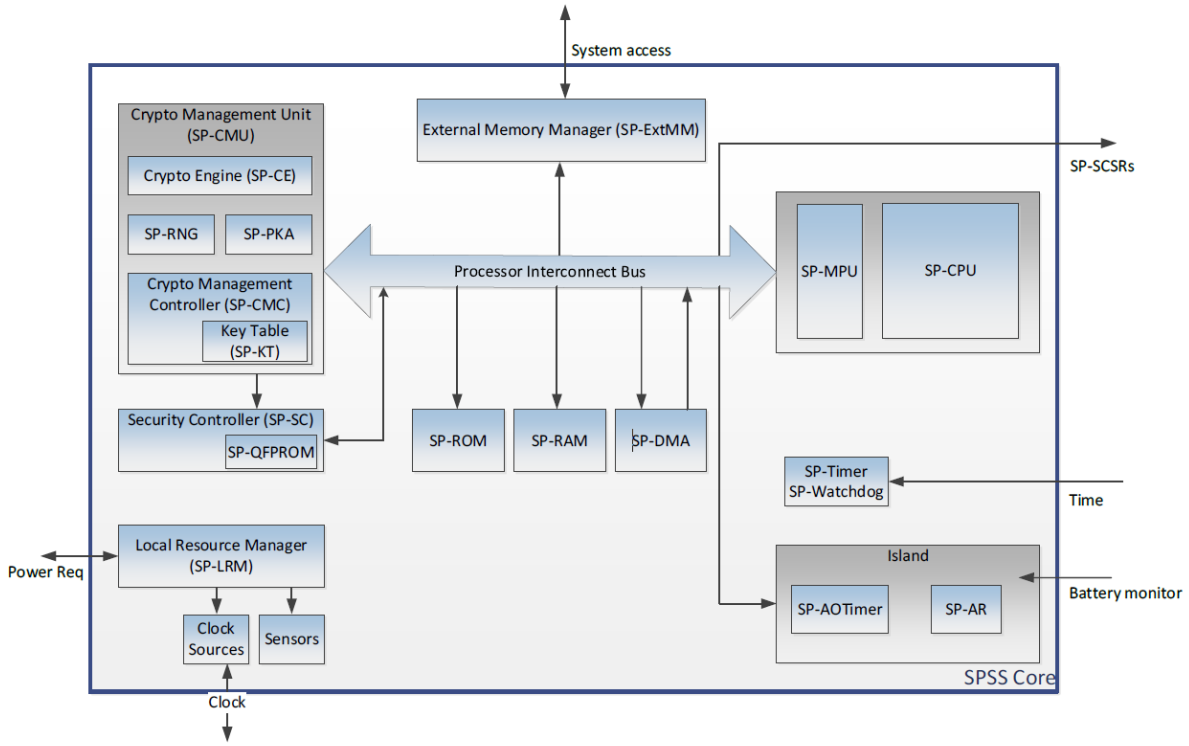
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 6.2 of the *[ST]*.

2.3.2 Clarification of scope

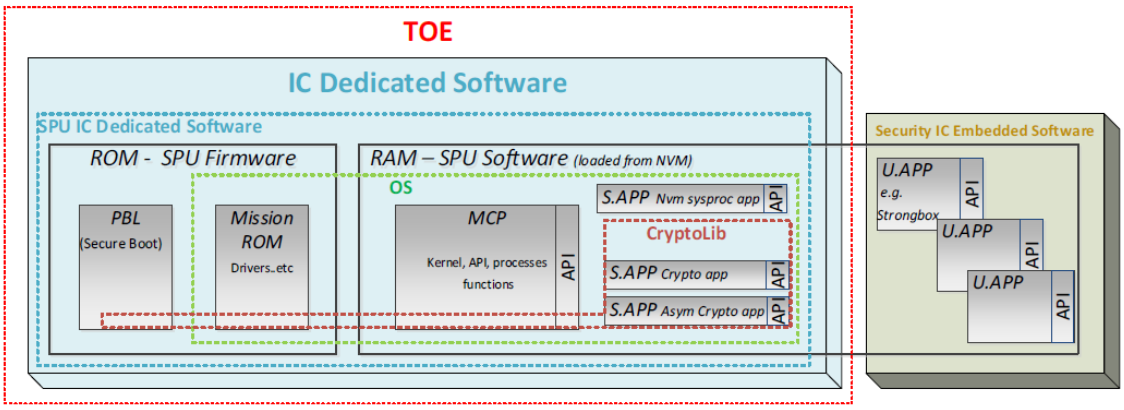
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

The following figure depicts the main HW TOE architecture.



The figure below depicts the IC Dedicated Software block decomposition of the TOE.



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 SM8650	80-40938-16, Revision AB
SM8650/SM8650P Secure Boot Enablement	80-40939-42, Revision AB
SM8650/SM8650P Qualcomm® Secure Processing Unit Enablement – User Guide	80-40939-150, Revision AD
SM8650/SM8650P Security Guidance for Secure Processing Unit Application Developers	80-40939-152, Revision AE

SM8650 Secure Processor Unit SDK – API Reference	80-PV579-31, Revision AC
Qualcomm® Snapdragon™ Secure Processing Unit (SPU) Application Development User Guide	80-NU430-7, Rev. 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 total test effort expended by the evaluators during the baseline evaluation was 29 weeks. During that test campaign, 7% of the total time was spent on Physical attacks, 29% on Characterisation tests, 24% on Perturbation attacks, and 40% on side-channel testing. No testing was carried out during this evaluation as it was all reused.

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. The evaluator verified that testing on Test OS provides the targeted security functionalities and environment which are representative of the TOE configuration and countermeasures.

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

This is a re-certification. Documentary evaluation results from the baseline evaluation have been reused, but vulnerability analysis and penetration testing has been renewed.

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

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Qualcomm Secure Processor Unit SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support.

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]*[3]. 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 SPU280 (Version: 7.0) in SM8650 SoC (Qualcomm® Snapdragon™ 8 Gen 3) with symmetric and asymmetric crypto support, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented with ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

[3] 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.

The Security Target claims 'strict' 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).

3 Security Target

The Qualcomm SPU280 Security Target for EAL5+, 80-NU430-13 Rev. AD, March 13 2024 *[ST]* is included here by reference.

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

4 Definitions

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

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

5 Bibliography

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

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[COMP]	Joint Interpretation Library, Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018
[ETR]	Evaluation Technical Report for Qualcomm Secure Processor Unit SPU280 (Version: 7.0) in SM8650 SoC with symmetric and asymmetric crypto support, 32330033-D3, version 1.2, 16 April 2024.
[ETRfC]	ETR for composite evaluation Qualcomm Secure Processor Unit SPU280 (Version: 7.0) in SM8650 SoC with symmetric and asymmetric crypto support, 2330033-D4, version 1.2, 16 April 2024.
[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_0084]	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 SPU280 Security Target for EAL5+, 80-NU430-13 Rev. AD, March 13 2024
[ST-lite]	Qualcomm SPU280 Security Target Lite for EAL5+, 80-NU430-14 Rev. AD, March 13 2024
[ST-SAN]	ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006
[STAR]	Site Technical Audit Report for Qualcomm, COMET Taiwan, 2330033-D16, version 1.1, 27 March 2024.

(This is the end of this report.)