Qualcomm® Crypto Engine Core

Module versions 5.7.0, 5.7.2 and 5.7.3

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.1

Last update: 07-08-2024

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

www.atsec.com

1 Table of Contents

1 General

1.1 This Security Policy Document

This Security Policy describes the features and design of the module named Qualcomm® Crypto Engine Core [1] using the terminology contained in the FIPS 140-3 specification. The FIPS 140-3 Security Requirements for Cryptographic Modules specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information. The NIST/CCCS Cryptographic Module Validation Program (CMVP) validates cryptographic modules to FIPS 140-3. Validated products are accepted by the Federal agencies of both the USA and Canada for the protection of sensitive or designated information.

1.2 How this Security Policy was Prepared

In preparing the Security Policy document, the laboratory formatted the vendor-supplied documentation for consolidation without altering the technical statements therein contained. The further refining of the Security Policy document was conducted iteratively throughout the conformance testing, wherein the Security Policy was submitted to the vendor, who would then edit, modify, and add technical contents. The vendor would also supply additional documentation, which the laboratory formatted into the existing Security Policy, and resubmitted to the vendor for their final editing.

This document is the non-proprietary FIPS 140-3 Security Policy for versions 5.7.0, 5.7.2 and 5.7.3 of the Qualcomm Crypto Engine Core. It has a one-to-one mapping to the [SP 800-140B] starting with section B.2.1 named “General” that maps to section 1 in this document and ending with section B.2.12 named “Mitigation of other attacks” that maps to section 12 in this document.

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	N/A
6	Operational Environment	N/A
7	Physical Security	2
8	Non-invasive Security	N/A
9	Sensitive Security Parameter Management	1

[1] Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.

10	Self-tests	1
11	Life-cycle Assurance	2
12	Mitigation of Other Attacks	N/A
Overall		1

Table 1 - Security Levels

2 Cryptographic Module Specification

2.1 Description of Module

The Qualcomm Crypto Engine Core cryptographic module is a sub-chip hardware module in a single chip embodiment for the purpose of FIPS 140-3 validation.

The Qualcomm Crypto Engine Core has been tested on the following platforms with the corresponding module variants and configuration options:

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
Snapdragon®[2] 8 Gen 2 Mobile Platform	Qualcomm Crypto Engine Core with version 5.7.0	N/A	N/A
Qualcomm® QCM4490	Qualcomm Crypto Engine Core with version 5.7.3	N/A	N/A
Qualcomm® QCS4490	Qualcomm Crypto Engine Core with version 5.7.3	N/A	N/A
Snapdragon® 4 Gen 2 Mobile Platform	Qualcomm Crypto Engine Core with version 5.7.3	N/A	N/A
Snapdragon® XR2 Gen 2 Platform	Qualcomm Crypto Engine Core with version 5.7.2	N/A	N/A

Table 2 - Cryptographic Module Tested Configuration

The table below lists all security functions of the module, including specific key strengths employed for approved services, and implemented modes of operation.

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2908 #A3694 #A4464	AES FIPS 197 SP-800-38A	CBC, CTR and ECB	128 and 256 bits	encryption/decryption
#A2908 #A3694 #A4464	AES-XTS SP-800-38E	XTS	128 and 256 bits	encryption/decryption
#A2908 #A3694 #A4464	AES-CCM SP-800-38C	CCM	128 and 256 bits	encryption/decryption

[2] Snapdragon is a product of Qualcomm Technologies, Inc. and/or its subsidiaries.

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2908 #A3694 #A4464	AES-CMAC SP-800-38B	CMAC	128 and 256 bits	message authentication code
#A2908 #A3694 #A4464	HMAC FIPS 198-1	SHA-1, SHA-256, SHA-384, SHA-512	512 bits with 256 bits of strength	message authentication code
#A2908 #A3694 #A4464	SHA FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512	N/A	hash

Table 3 - Approved Algorithms

Algorithm/Functions	Use/Function
AES-GCM	encryption, decryption
DES CBC	encryption, decryption
DES ECB	encryption, decryption
Triple-DES	encryption, decryption
HMAC SHA-1 with key size other than 512 bits	message authentication code
HMAC SHA-256 with key sizes other than 512 bits	message authentication code
HMAC SHA-384 with key sizes other than 512 bits	message authentication code
HMAC SHA-512 with key sizes other than 512 bits	message authentication code
AEAD-SHA-1 AES CBC	encryption, decryption (with message authentication code)
AEAD-SHA-1 AES CTR	encryption, decryption (with message authentication code)
AEAD-SHA-1 DES CBC	encryption, decryption (with message authentication code)

AEAD-SHA-1 Triple-DES CBC	encryption, decryption (with message authentication code)
SM3	hashing
SM4	encryption, decryption

Table 4 - Non-Approved Not Allowed in the Approved Mode of Operation

2.2 Cryptographic Module Boundary

The cryptographic boundary of the Qualcomm Crypto Engine Core is represented by the blue box. The module has been tested on the Snapdragon 8 Gen 2 Mobile Platform SoC, Qualcomm QCM4490 SoC, Qualcomm QCS4490 SoC, Snapdragon 4 Gen 2 Mobile Platform SoC, and Snapdragon XR2 Gen 2 Platform SoC which forms the physical perimeter for the module.

Below is an illustrative diagram.

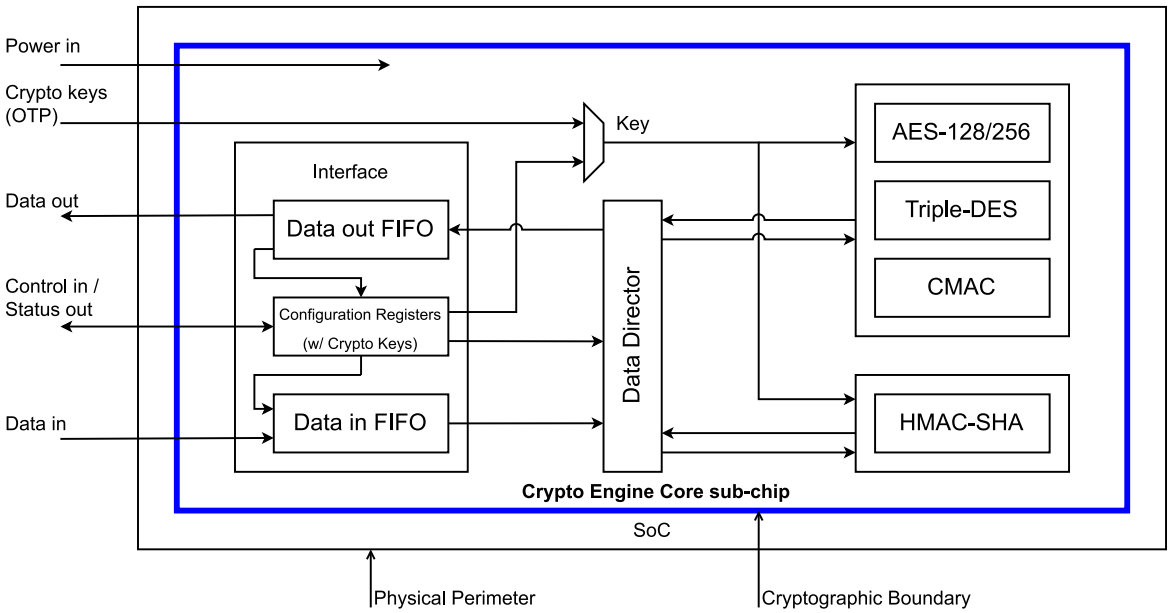

Figure 1 - Hardware Block Diagram

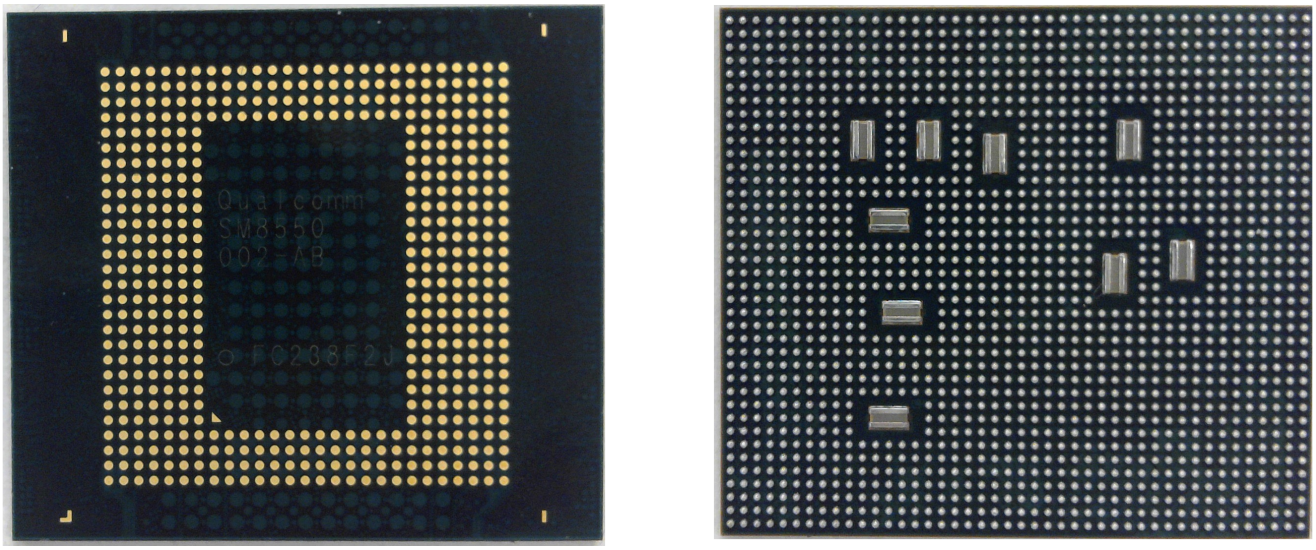

Figure 2: Snapdragon 8 Gen 2 Mobile Platform

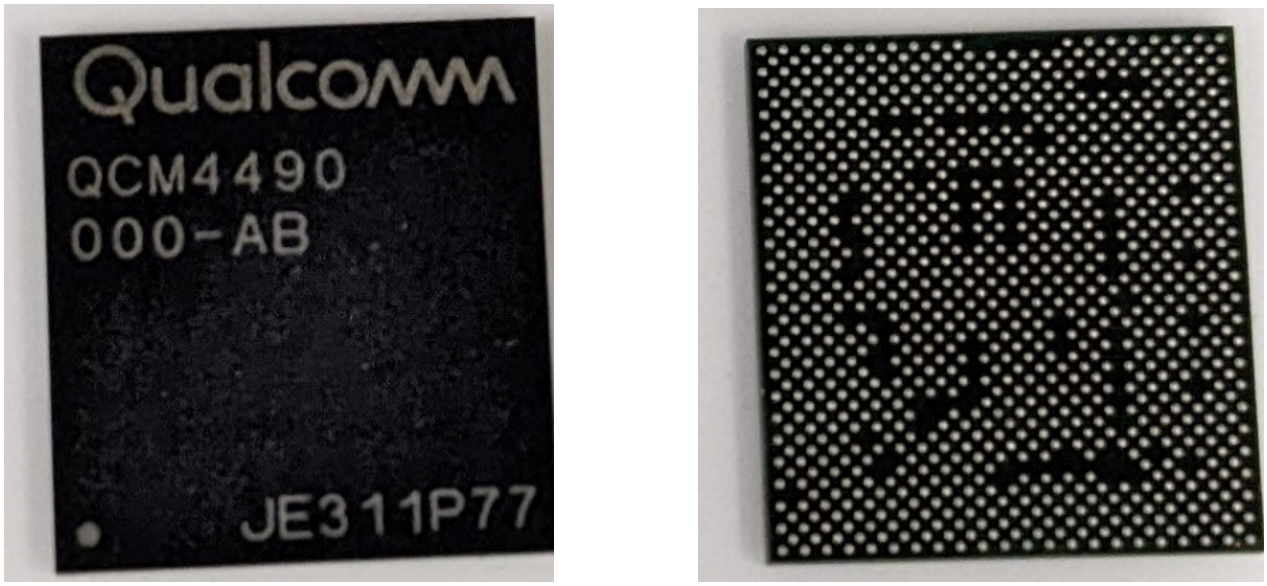

Figure 3 - Qualcomm QCM4490

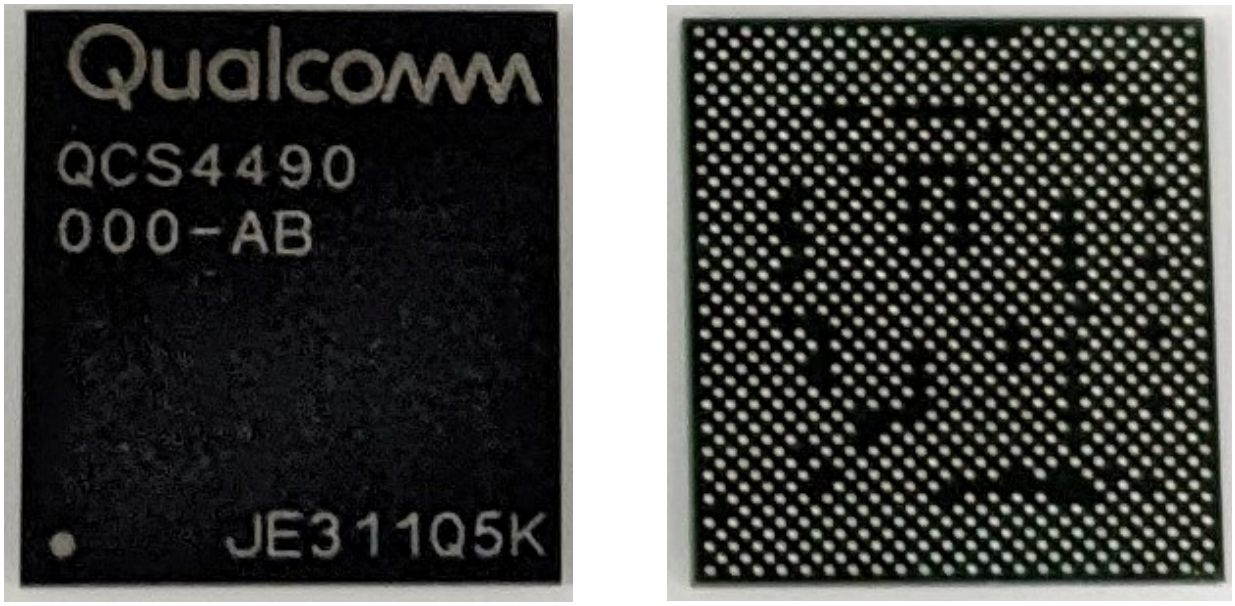

Figure 4 - Qualcomm QCS4490

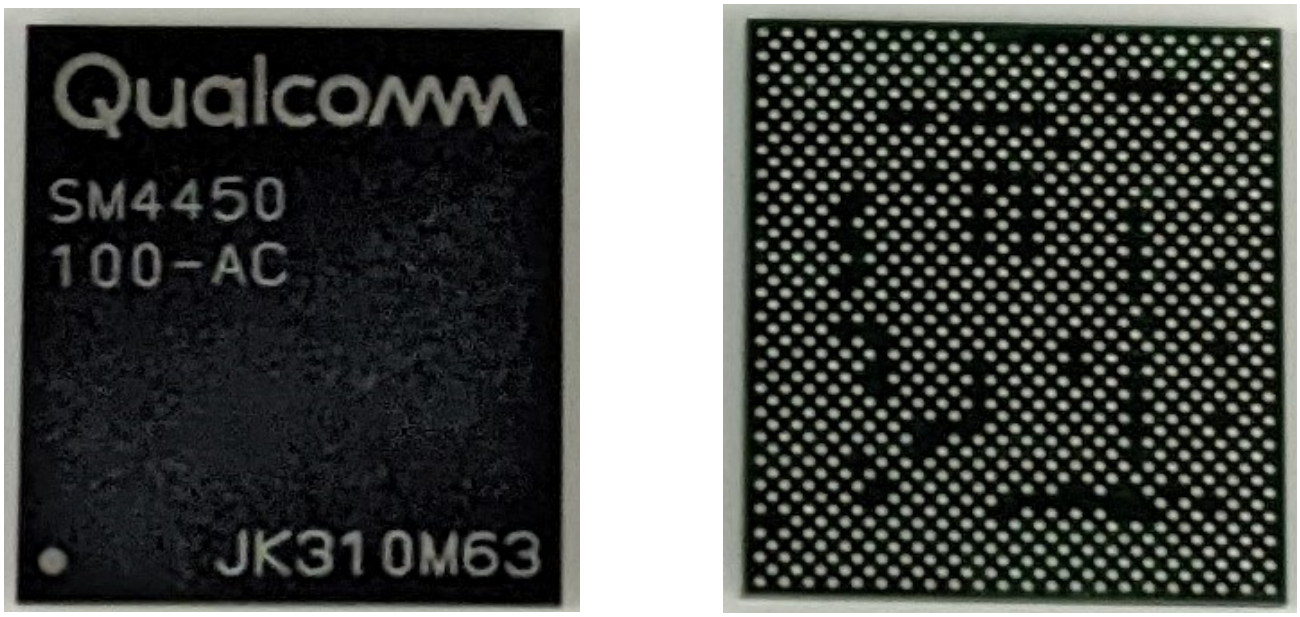

Figure 5 – *Snapdragon 4 Gen 2 Mobile Platform*

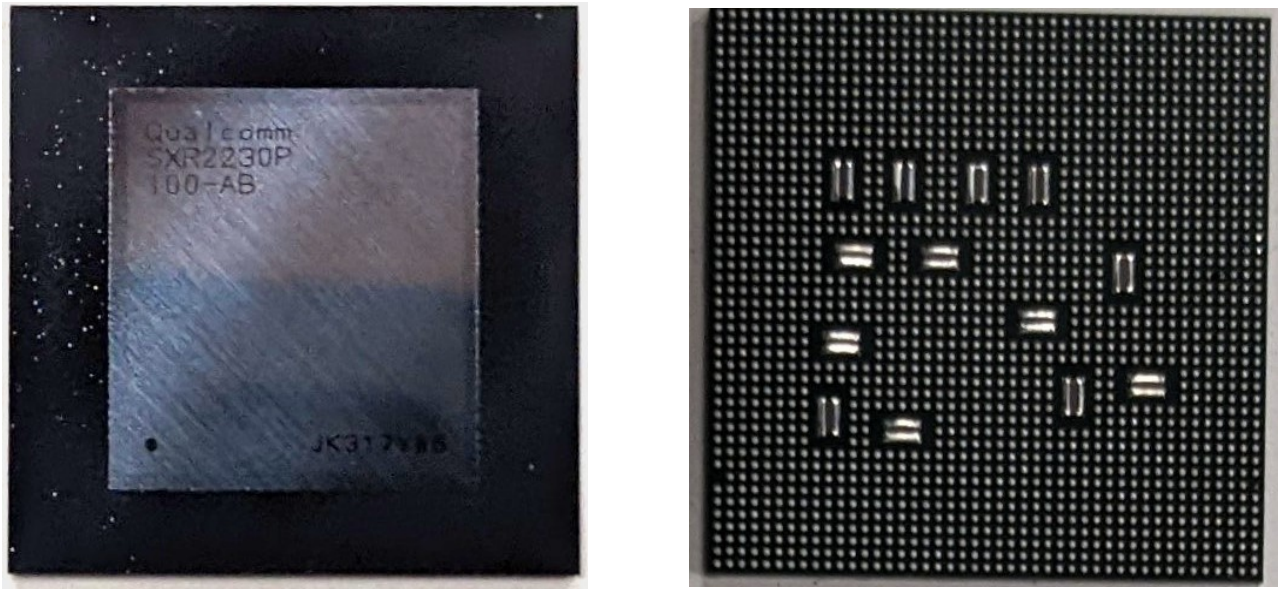

Figure 6 – *Snapdragon XR2Gen 2Platform*

The tested operational environment's physical perimeter (TOEPP) is the entire single chip.

2.3 Description of Modes of Operations

The Qualcomm Crypto Engine Core supports two modes of operation: approved mode and a non-approved mode. The switching of modes of operation is implicit depending on the service invoked, but the approved services are explicitly identified by an indicator. The Qualcomm Crypto Engine Core enters approved mode after successful completion of the conditional algorithm self-tests. When the operator invokes a non-approved service, the Qualcomm Crypto Engine Core implicitly switches to its non-approved mode. If the module is in the non-approved mode of operation and

the operator requests an approved service, the Qualcomm Crypto Engine Core implicitly switches to its approved mode. All CSPs are kept separate between the two modes.

3 Cryptographic Module Ports and Interfaces

Physical port	Logical Interface	Data that passes over port/interface
Data In FIFO, registers	Data Input	All input data
Data Out FIFO	Data Output	All data output except Status information
Registers	Control Input	Command input
Registers	Status Output	Status information
Physical power connector	Power Input	Power from SoC power port

Table 5 - Ports and Interfaces

All status ports and control ports are directed through the interface of the Qualcomm Crypto Engine Core cryptographic boundary. The registers of the Qualcomm Crypto Engine Core are used for control input and status output interfaces. Qualcomm Crypto Engine Core FIFOs are implemented to provide the high-speed interfaces for data input and data output. The Qualcomm Crypto Engine Core does not implement a Control Output interface.

If a caller wants to use a non-Approved cipher, a separate “pipe pair” must be used or a new key for the non-Approved cipher must be loaded.

4 Roles, services, and authentication

4.1 Roles

The module only supports crypto Officer (CO) role that is assumed implicitly when a service is requested form the module.

Role	Service	Input	Output
Crypto Officer (CO)	AES Encryption	AES Key, Plaintext	Ciphertext, Success/Fail
	AES Decryption	AES Key, Ciphertext	Plaintext, Success/Fail
	CMAC Message Authentication	AES Key, Input data	CMAC value
	HMAC Message Authentication	HMAC Key, input data	HMAC value
	Hash	Input data	Hash value
	Self-Test	None	Self-test success/fail
	Zeroization	None	None
	Configure keys for use by CO	AES Key, HMAC Key	Success/Fail
	Status output	None	Current status (as return codes and/or log messages)
	Show version	None	Name and version information read from register CRYPTO0_CRYPTO_VERSION
	Encryption	DES Key, Triple-DES Key or SM4 Key, Plaintext	Ciphertext, Success/Fail
	Decryption	DES Key, Triple-DES Key or SM4 Key, Ciphertext	Plaintext, Success/Fail
	Message Authentication	HMAC Key with size that is not 512 bits, Input data	HMAC value
	Authenticated Encryption [AEAD]	AES Key or Triple-DES Key and input data	Ciphertext, Success/Fail
	Authenticated Decryption	AES Key or Triple-DES Key and input data	Plaintext, Success/Fail

Table 6 - Roles, Service Commands, Input and Output

4.2 Services

The Qualcomm Crypto Engine Core does not provide a bypass capability.

All services are implemented within the Qualcomm Crypto Engine Core. The service indicator CRYPTO0_CRYPTO_STATUS4 bits 16 – 29 will show zero for the approved services based on the register bit field for the service.

In Table 7, the convention below applies when specifying the access permissions (types) that the service has for each SSP:

G = **Generate**: The module generates or derives the SSP.
R = **Read**: The SSP is read from the module (e.g. the SSP is output).
W = **Write**: The SSP is updated, imported, or written to the module.
E = **Execute**: The module uses the SSP in performing a cryptographic operation.
Z = **Zeroize**: The module zeroizes the SSP.

The following table describes the services available in approved mode:

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
AES Encryption	Perform data encryption	AES CBC, CCM, CTR, XTS and ECB 128/256	AES Key	CO	E, W	CRYPTO0_CRYPTO_STATUS4 bits 16-18 set to 0
AES Decryption	Perform data decryption	AES CBC, CCM, CTR, XTS and ECB 128/256			E, W	
CMAC Message Authentication	Message Authentication	CMAC-AES 128/256			E, W	CRYPTO0_CRYPTO_STATUS4 bit 29 set to 0
HMAC Message Authentication		HMAC using SHA-1, SHA-256, SHA-384, SHA-512	HMAC Key (with 512-bit key length)		E, W	CRYPTO0_CRYPTO_STATUS4 bits 25-28 set to 0
Hash	Hashing	SHA-1, SHA-256, SHA-384, SHA-512	N/A		N/A	CRYPTO0_CRYPTO_STATUS4 bits 21-24 set to 0
Self-Test	Self-Tests are executed automatically when device is booted or restarted	None			N/A	None
Zeroization	Zeroizes all SSP	None	AES key or HMAC key		Z	None
Configure keys for use by Crypto Officer	Configures the keys for Crypto Officer role	None	AES Key and HMAC Key	CO	W	None

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Status output	Show status of the module state	None	N/A	CO	N/A	None
Show version	Show the version and name of the module	None	N/A	CO	N/A	None

Table 7 - Approved Services

The following table describes the services available in Non-approved mode:

Service	Description	Algorithms Accessed	Role	Indicator
Encryption	Encrypts data using symmetric cryptography	DES, Triple-DES, AES-GCM, SM4	CO	None
Decryption	Decrypts data using symmetric cryptography	DES, Triple-DES, AES-GCM, SM4		None
Hash	Hashing algorithm	SM3		None
Message Authentication	Computes the MAC value of data	HMAC (key sizes other than 512 bits)		None
Authenticated Encryption [AEAD]	Encrypts data using symmetric cryptography	AEAD-SHA-1 AES CBC, AEAD-SHA-1 AES CTR, AEAD-SHA-1 DES CBC, AEAD-SHA-1 Triple-DES CBC		None
Authenticated Decryption	Decrypts data using symmetric cryptography	AEAD-SHA-1 AES CBC, AEAD-SHA-1 AES CTR, AEAD-SHA-1 DES CBC, AEAD-SHA-1 Triple-DES CBC		None

Table 8 - Non-Approved Services

4.3 Operator Authentication

There is no operator authentication; assumption of role is implicit by the used service(s).

5 Software/Firmware security

The Qualcomm Crypto Engine Core does not support any software or firmware component. Therefore, this section is not applicable.

6 Operational Environment

6.1 Applicability

The Qualcomm Crypto Engine Core is a single-chip hardware module with a non-modifiable operational environment. The procurement, build and configuring procedure are controlled by the Vendor.

7 Physical Security

The Qualcomm Crypto Engine Core Cryptographic Module is a single-chip hardware module which conforms to the Level 2 requirements for physical security. The Qualcomm Crypto Engine Core is a sub-chip that is enclosed within production grade components.

At the time of manufacturing, the die containing the Qualcomm Crypto Engine Core is embedded within a printed circuit board (PCB), which prevents visibility into the internal circuity of the Qualcomm Crypto Engine Core. The layering process which embeds the die into the PCB prevents tampering of the physical components without leaving tamper evidence.

The Qualcomm Crypto Engine Core is further protected by being enclosed in a commercial off-the-shelf mobile device which is itself made with production grade commercially available components. This mobile device enclosure completely surrounds the Qualcomm Crypto Engine Core.

There are no steps required to ensure that physical security is maintained.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper evident coating	N/A	N/A

Table 9 - Physical Security Inspection Guidelines

8 Non-invasive Security

The Qualcomm Crypto Engine Core does not support any non-invasive security techniques. Therefore, this section is not applicable.

9 Sensitive Security Parameter Management

9.1 SSP List

Table 10 below lists the SSPs used within the Qualcomm Crypto Engine Core.

Key/SSP Name /Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establish-ment	Storage	Zero-ization	Use and related keys
AES Key (CSP)	128 or 256 bits	AES AES-CMAC #A2908 #A3694 #A4464 AES Modes: AES-CBC, AES-CCM, AES-CTR, AES-XTS, AES-ECB,	N/A	Import: Provided by caller. Export: N/A	N/A	Hardware registers	Zeroized during module reset	Encryption and decryption and Message Authenti-cation
HMAC Key (CSP)	256 bits	HMAC #A2908 #A3694 #A4464	N/A	Import: Provided by caller. Export: N/A	N/A	Hardware registers	Zeroized during module reset	Message Authenti-cation

Table 10 – SSPs

9.2 SSP Generation

The Qualcomm Crypto Engine Core does not perform SSP generation for any algorithms.

9.3 SSP Entry and Output

The module does not provide SSP entry or output services. Instead, SSPs are provided from the caller within the tested operation environment’s physical perimeter (TOEPP) hardware via a single-chip TOEPP path, which is not considered SSP establishment by Table 1 of FIPS 140-3 IG 9.5.A. SSPs can only be written to the Qualcomm Crypto Engine Core by the boot loader by writing to the key registers or into the FIFOs assigned to the particular use case.

Any attempt to write to a non-assigned FIFO is blocked. The Qualcomm Crypto Engine Core ensures that there is no means to obtain CSP or key data from the Qualcomm Crypto Engine Core by placing the CSPs into write-only registers. This action prevents an entity interacting with the Qualcomm Crypto Engine Core from being able to read the CSPs.

9.4 SSP Storage

The Qualcomm Crypto Engine Core stores all SSPs internally (the storage is non-persistent). In addition, all SSPs are stored write-only and are not readable outside of the Qualcomm Crypto Engine Core. Therefore, any attempt to read SSPs are blocked by the Qualcomm Crypto Engine Core control logic, which will return zeros instead of an SSP.

9.5 SSP Zeroization

When the Qualcomm Crypto Engine Core receives a reset event, it will zeroize all SSPs contained within the FIPS 140-3 Non-Proprietary Security Policy. The registers for the SSPs are set to zero during power-off, indicating implicitly that SSP zeroization was successful.

10 Self-tests

Cryptographic algorithm self-tests (CASTs) are automatically performed during power-up of the Qualcomm Crypto Engine Core. During CAST execution, no services are available, and input and output are inhibited by the Qualcomm Crypto Engine Core control logic.

10.1 Pre-Operational Tests

The Qualcomm Crypto Engine Core is solely implemented in hardware and does not have any software or firmware components. As such, the module does not perform any pre-operational software/firmware integrity test. Instead, the module performs the CASTs listed in Table 11 as the pre-operational self-test.

The Qualcomm Crypto Engine Core does not implement a pre-operational bypass test nor pre-operational critical functions test.

10.2 Conditional Self-Tests

The Qualcomm Crypto Engine Core conditional self-tests are CASTs and have been listed in Table 11. These CASTs are executed during each power-on.

The Qualcomm Crypto Engine Core does not implement a Software/Firmware Load Test, Manual Entry Test, Conditional Bypass Test, or a Conditional Critical Functions Test.

Algorithm	Key Size	Test
AES encryption (CCM)	256 bits	Known Answer Test (KAT)
AES decryption (CCM)	256 bits	KAT
AES encryption (ECB)	256 bits	KAT
AES decryption (ECB)	256 bits	KAT
HMAC SHA-1/SHA-256/SHA-384/SHA-512	512 bits	KAT
AES-CMAC MAC generation and verification	256 bits	KAT

Table 11 - Conditional Cryptographic Algorithm Self-Tests

10.3 On-Demand Self-Tests

The operator may invoke self-tests on-demand by powering-off and reloading the Qualcomm Crypto Engine Core. During the execution of the on-demand self-tests, no cryptographic services are available, and no data output or input is possible.

10.4 Error States

Table 12 below lists the causes that trigger the Qualcomm Crypto Engine Core to enter its error state. When entering its error state, the Qualcomm Crypto Engine Core sets the BIST_FAILURE register to indicate that it is in the error state. While in the error state, all data input and output are prohibited and no further cryptographic operation is allowed. The Qualcomm Crypto Engine

Core control logic enforces this prohibition by preventing external usage while the module is in the error state. In addition, neither caller-induced nor internal errors reveal any sensitive material to callers.

Once the Qualcomm Crypto Engine Core is in the error state, it will only respond to a reset command. A reset will cause the Qualcomm Crypto Engine Core to re-execute its CASTs. The Qualcomm Crypto Engine Core will remain unavailable until it passes its CASTs.

Error State	Cause of Error	Status Indicator
Error	KAT failure	BIST_FAILURE indicator is set

Table 12 - Error States

11 Life-cycle assurance

11.1 Delivery and Operation

The Qualcomm Crypto Engine Core is a sub-chip module that runs on the Snapdragon 8 Gen 2 Mobile Platform SoC, Qualcomm QCM4490 SoC, Qualcomm QCS4490 SoC, Snapdragon 4 Gen 2 Mobile Platform SoC, and Snapdragon XR2 Gen 2 Platform SoC. The vendor uses a trusted delivery courier to transport the SoC to their customers. On the reception of the SoC, the operator shall first check all sides of the box to verify that it has not been tampered with during the shipment. Then, after opening the box the operator shall verify that the moisture barrier bag is still sealed and does not present any trace of tampering. Finally, after retrieving the SoC, the operator shall perform a visual inspection of the external package of the module; it should look similar to the picture in Figure 2. If one of these verifications fail, the operator shall contact their Qualcomm Technologies' representative who released the delivery before operating the module.

Once the product is received by the customer and powered up, the tests defined in Table 11 will be executed.

11.2 End of Life

Because the module does not have persistent storage, all SSPs are zeroized and the module is securely sanitized when powered down. Thus, the module may be distributed to other operators or disposed of after each power off.

11.3 Crypto Officer Guidance

The operation of the Qualcomm Crypto Engine Core does not need FIPS 140-3 specific guidance. The FIPS 140-3 functional requirements are always met.

For using the cryptographic services of the Qualcomm Crypto Engine Core, the manual for the Qualcomm Crypto Engine Core covers the description of the register set as well as the use of the FIFOs channels should be used.

NOTE:

- The module ensures that the AES algorithm in XTS mode is only used for the cryptographic protection of data on storage devices, as specified in [SP800-38E]. The module does not support AES-XTS data units longer than 2^{20} AES blocks. In compliance with IG C.I, the module performs a check to ensure that the two AES-XTS keys are different.

11.4 Configuration Management

ClearCase, a version control system from IBM/Rational, is used to manage the revision control of the hardware code (Verilog code) and hardware documentation. The ClearCase version control system provides version control, workspace management, parallel development support and build auditing. The Verilog code is maintained within the ClearCase database used by Qualcomm Technologies, Inc.

12 Mitigation of other attacks

The Qualcomm Crypto Engine Core does not implement security mechanisms to mitigate other attacks.

Appendix A. Glossary and Abbreviations

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CAST	Cryptographic Algorithm Self-test
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block-chaining
CCCS	Canadian Centre for Cyber Security
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
CTR	Counter Mode
DES	Data Encrypted Signature
ECB	Electronic Code Book
FIFO	First-in First-out (Queue)
FIPS	Federal Information Processing Standards Publication
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
PCB	Printed Circuit Board
SHA	Secure Hash Algorithm
SoC	System on a Chip
SSP	Sensitive Security Parameter
TDES	Triple-DES
TOEPP	Trusted Operating Environment Physical Perimeter
XTS	XEX-based Tweaked-codebook mode with cipher text Stealing

Appendix B. References

FIPS140-3 **FIPS PUB 140-3 - Security Requirements For Cryptographic Modules**
March 2019
https://doi.org/10.6028/NIST.FIPS.140-3

FIPS140-3_IG **Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program**
March 2023
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

FIPS180-4 **Secure Hash Standard (SHS)**
August 2015
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

FIPS197 **Advanced Encryption Standard**
November 2001
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

FIPS198-1 **The Keyed Hash Message Authentication Code (HMAC)**
July 2008
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf

SP800-38A **NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP800-38B **NIST Special Publication 800-38B - Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication**
October 2016
http://csrc.nist.gov/publications/nistpubs/800-38B/SP_800-38B.pdf

SP800-38C **NIST Special Publication 800-38C - Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality**
July 2007
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

SP800-38D **NIST Special Publication 800-38D - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**
November 2007
http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

SP800-38E **NIST Special Publication 800-38E - Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices**
January 2010
http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

SP800-67r2 **NIST Special Publication 800-67 Revision 2 - Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher**
November 2017
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf

SP800-140B **NIST Special Publication 800-140B - CMVP Security Policy Requirements**
March 2020
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140B.pdf