Qualcomm Technologies, Inc.

Qualcomm(R) Crypto Engine Core

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Last Update: 09-04-2025

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

https://www.atsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

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 Security Levels

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
10	Self-tests	1
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

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.

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use: 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 module is a general-purpose engine that provides cryptographic services (as listed in Section 4.3) to the components residing within the same operational environment which act as operators. These operators can request module services using FIFOs and registers.

Module Type: Hardware

Module Embodiment: SingleChip

Module Characteristics: SubChip

Cryptographic Boundary:

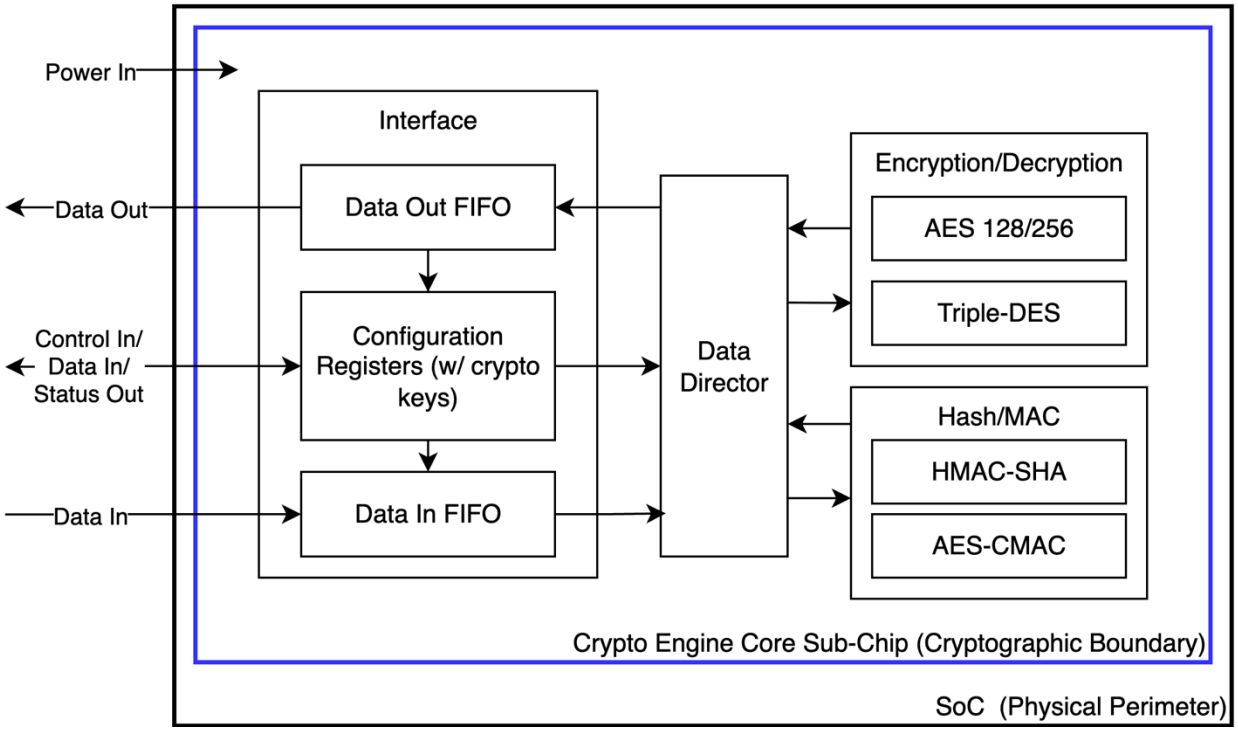

Figure 1: Cryptographic boundary and physical perimeter

Tested Operational Environment's Physical Perimeter (TOEPP):

The tested operational environment's physical perimeter is the single chip.

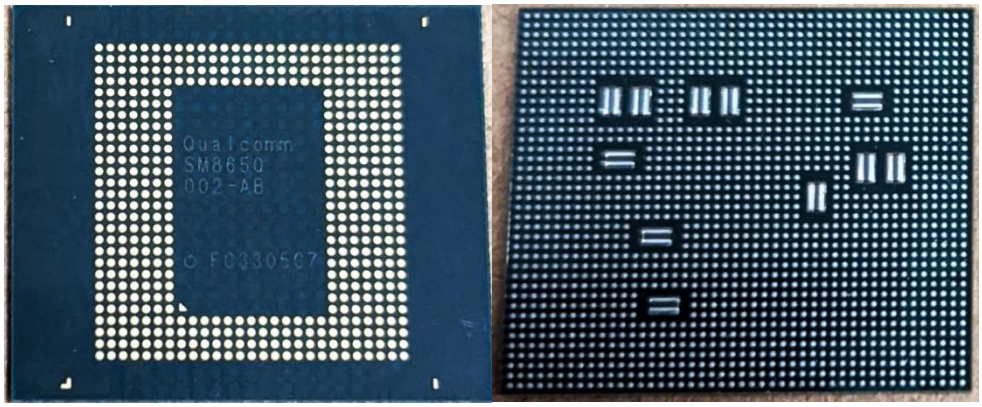

Figure 2: Snapdragon 8 Gen 3 Mobile Platform

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Snapdragon® 8 Gen 3 Mobile Platform	5.8.0	N/A	Snapdragon® 8 Gen 3 Mobile Platform	N/A

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

There are no excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode of operation	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service
Non-approved mode of operation	Automatically entered whenever a non-approved service is requested	Non-Approved	Non-approved services are not explicitly indicated. The absence of an explicit indicator is an implicit indicator of non-approved services.

Table 3: Modes List and Description

The Qualcomm® Crypto Engine Core supports two modes of operation: approved mode and a non-approved mode. All CSPs are kept separate between the two modes through the use of a key policy management system.

Mode Change Instructions and Status:

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 the 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.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A4289	-	SP 800-38A
AES-CCM	A4289	-	SP 800-38C
AES-CMAC	A4289	-	SP 800-38B
AES-CTR	A4289	-	SP 800-38A
AES-ECB	A4289	-	SP 800-38A
AES-XTS Testing Revision 2.0	A4289	-	SP 800-38E
HMAC-SHA-1	A4289	-	FIPS 198-1
HMAC-SHA2-256	A4289	-	FIPS 198-1
HMAC-SHA2-384	A4289	-	FIPS 198-1
HMAC-SHA2-512	A4289	-	FIPS 198-1
HMAC-SHA3-224	A4289	-	FIPS 198-1
HMAC-SHA3-256	A4289	-	FIPS 198-1
HMAC-SHA3-384	A4289	-	FIPS 198-1
HMAC-SHA3-512	A4289	-	FIPS 198-1
SHA-1	A4289	-	FIPS 180-4
SHA2-256	A4289	-	FIPS 180-4
SHA2-384	A4289	-	FIPS 180-4
SHA2-512	A4289	-	FIPS 180-4
SHA3-224	A4289	-	FIPS 202
SHA3-256	A4289	-	FIPS 202
SHA3-384	A4289	-	FIPS 202
SHA3-512	A4289	-	FIPS 202

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES-GCM	encryption, decryption
DES-CBC	encryption, decryption
DES-ECB	encryption, decryption
TDES (two independent keys)	encryption, decryption
TDES (three independent keys)	encryption, decryption
HMAC SHA-1 with key size other than 512 bits	message authentication code
HMAC SHA2-256 with key sizes other than 512 bits	message authentication code
HMAC SHA2-384 with key sizes other than 512 bits	message authentication code
HMAC SHA2-512 with key sizes other than 512 bits	message authentication code
HMAC SHA3-224 with key sizes other than 512 bits	message authentication code
HMAC SHA3-256 with key sizes other than 512 bits	message authentication code
HMAC SHA3-384 with key sizes other than 512 bits	message authentication code
HMAC SHA3-512 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 TDES-CBC	encryption, decryption (with message authentication code)
SM3	hashing
SM4	encryption, decryption

Table 5: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES-CBC	BC-UnAuth	AES in CBC mode	Reference:FIPS 197, SP800-38A	AES-CBC: (A4289)
AES-CCM	BC-Auth	AES in CCM mode	Reference:FIPS 197, SP800-38C	AES-CCM: (A4289)
AES-CMAC	MAC	AES in CMAC mode	Reference:FIPS 197, SP800-38B	AES-CMAC: (A4289)
AES-CTR	BC-UnAuth	AES in CTR mode	Reference:FIPS 197, SP800-38A	AES-CTR: (A4289)
AES-ECB	BC-UnAuth	AES in ECB mode	Reference:FIPS 197, SP800-38A	AES-ECB: (A4289)
AES-XTS	BC-UnAuth	AES in XTS mode	Reference:FIPS 197, SP800-38E	AES-XTS Testing Revision 2.0: (A4289)
HMAC-SHA-1	MAC	HMAC with SHA-1	Reference:FIPS 198-1, FIPS 180-4	HMAC-SHA-1: (A4289)
HMAC-SHA2-256	MAC	HMAC with SHA2-256	Reference:FIPS 198-1, FIPS 180-4	HMAC-SHA2-256: (A4289)
HMAC-SHA2-384	MAC	HMAC with SHA2-384	Reference:FIPS 198-1, FIPS 180-4	HMAC-SHA2-384: (A4289)
HMAC-SHA2-512	MAC	HMAC with SHA2-512	Reference:FIPS 198-1, FIPS 180-4	HMAC-SHA2-512: (A4289)
HMAC-SHA3-224	MAC	HMAC with SHA3-224	Reference:FIPS 198-1, FIPS 202	HMAC-SHA3-224: (A4289)
HMAC-SHA3-256	MAC	HMAC with SHA3-256	Reference:FIPS 198-1, FIPS 202	HMAC-SHA3-256: (A4289)
HMAC-SHA3-384	MAC	HMAC with SHA3-384	Reference:FIPS 198-1, FIPS 202	HMAC-SHA3-384: (A4289)
HMAC-SHA3-512	MAC	HMAC with SHA3-512	Reference:FIPS 198-1, FIPS 202	HMAC-SHA3-512: (A4289)
SHA-1	SHA	SHA-1	Reference:FIPS 180-4	SHA-1: (A4289)
SHA2-256	SHA	SHA2-256	Reference:FIPS 180-4	SHA2-256: (A4289)
SHA2-384	SHA	SHA2-384	Reference:FIPS 180-4	SHA2-384: (A4289)
SHA2-512	SHA	SHA2-512	Reference:FIPS 180-4	SHA2-512: (A4289)
SHA3-224	SHA	SHA3-224	Reference:FIPS 202	SHA3-224: (A4289)
SHA3-256	SHA	SHA3-256	Reference:FIPS 202	SHA3-256: (A4289)
SHA3-384	SHA	SHA3-384	Reference:FIPS 202	SHA3-384: (A4289)
SHA3-512	SHA	SHA3-512	Reference:FIPS 202	SHA3-512: (A4289)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES XTS

The AES algorithm in XTS mode is only used for the cryptographic protection of data on storage devices, in compliance with [SP800-38E].

The module ensures that the length of a single data unit encrypted with the XTS-AES does not exceed 2^{20} AES blocks, that is 16MB of data.

To meet the requirement stated in IG C.I, the module implements a check that ensures, before performing any cryptographic operation, that the two AES keys used in AES XTS mode are not identical.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

2.9 Key Generation

Not Applicable. The key generation is not implemented.

2.10 Key Establishment

Not Applicable. The key establishment is not implemented.

2.11 Industry Protocols

Not Applicable. There are no industry protocols implemented.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Data In FIFO	Data Input	Input data
Data Out FIFO	Data Output	All data output except Status information
Registers	Data Input Control Input	Cryptographic keys; command input
Registers	Status Output	Status information
Physical power connector	Power	Power from SoC power port

Table 7: Ports and Interfaces

The Qualcomm® Crypto Engine Core does not implement a Control Output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 8: Roles

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

4.3 Approved Services

The convention below applies when specifying the access permissions 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.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES Encryption	Perform data encryption	CRYPTO0_CRYPTO_STATUS4 bits 16-18 set to 0	AES Key, Plaintext	Ciphertext, Success/Fail	AES-CBC AES-CCM AES-CTR AES-ECB AES-XTS	Crypto Officer - AES key: W,E
AES Decryption	Perform data decryption	CRYPTO0_CRYPTO_STATUS4 bit 29 set to 0	AES Key, Ciphertext	Plaintext, Success/Fail	AES-CBC AES-CCM	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					AES-CTR AES-ECB AES-XTS	- AES key: W,E
CMAC Message Authentication	Message Authentication	CRYPTO0_CRYPTO_STATUS4 bit 29 set to 0	AES Key, Input data	CMAC value	AES-CMAC	Crypto Officer - AES key: W,E
HMAC Message Authentication	Message Authentication	CRYPTO0_CRYPTO_STATUS4 bits 25-28 set to 0	HMAC Key, input data	HMAC value	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-	Crypto Officer - HMAC key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHA3-512	
Hash	Hashing	CRYPTO0_CRYPTO_STATUS4 bits 21-24 set to 0	Input data	Hash output	SHA-1 SHA2-256 SHA2-384 SHA2-512 SHA3-224 SHA3-256 SHA3-384 SHA3-512	Crypto Officer
Self-Test	Self-Tests are executed automatically when device is booted or restarted	None	None	Self-test Success/Fail	None	Crypto Officer - AES key: E - HMAC key: E
Zeroization	Zeroizes all SSPs	None	None	None	None	Crypto Officer - AES key: Z - HMAC key: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Configure keys for use by Crypto Officer	Configures the keys for Crypto Officer role	None	AES Key, HMAC Key, Triple-DES Key	Success/Fail	None	Crypto Officer - AES key: W - HMAC key: W
Show Status	Show status of the module state	None	None	Current status (as return codes and/or log messages)	None	Crypto Officer
Show version	Show the version and name of the module	None	None	Name and version information read from register CRYPTO0_CRYPTO_VERSION	None	Crypto Officer

Table 9: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Encryption	Encrypts data using symmetric cryptography	AES-GCM DES-CBC DES-ECB TDES (two independent keys) TDES (three independent keys) SM4	CO
Decryption	Decrypts data using symmetric cryptography	AES-GCM DES-CBC DES-ECB TDES (two independent keys) TDES (three independent keys) SM4	CO
Hash	Hashing algorithm	SM3	CO

Name	Description	Algorithms	Role
Message Authentication	Computes the MAC value of data	HMAC SHA-1 with key size other than 512 bits HMAC SHA2-256 with key sizes other than 512 bits HMAC SHA2-384 with key sizes other than 512 bits HMAC SHA2-512 with key sizes other than 512 bits HMAC SHA3-224 with key sizes other than 512 bits HMAC SHA3-256 with key sizes other than 512 bits HMAC SHA3-384 with key sizes other than 512 bits HMAC SHA3-512 with key sizes other than 512 bits	CO
Authenticated Encryption/Decryption [AEAD]	Encrypts or decrypts data using symmetric cryptography	AEAD-SHA-1 AES-CBC AEAD-SHA-1 AES-CTR AEAD-SHA-1 DES-CBC AEAD-SHA-1 TDES-CBC	CO

Table 10: Non-Approved Services

4.5 External Software/Firmware Loaded

Not Applicable. No external software or firmware is loaded.

5 Software/Firmware Security

5.1 Integrity Techniques

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper evident coating	N/A	N/A

Table 11: Mechanisms and Actions Required

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.

8 Non-Invasive Security

8.1 Mitigation Techniques

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Hardware register	Temporary storage for SSPs used by the module as part of service execution	Dynamic
Hardware FIFO	Temporary storage for SSPs used by the module as part of service execution	Dynamic

Table 12: Storage Areas

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.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input parameter	Caller within the physical perimeter	Hardware registers, hardware FIFOs	Plaintext	N/A	N/A	

Table 13: SSP Input-Output Methods

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.

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Power-off	All SSPs will be zeroized	The registers holding the SSPs are set to all zeroes	Operator can initiate this zeroization method by powering off the module

Table 14: SSP Zeroization Methods

The successful power-off of the module is an implicit indicator that zeroization has completed.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	Symmetric key used for encryption, decryption, and message authentication	128 or 256 bits - 128 or 256 bits	Symmetric key - CSP			AES-CBC AES-CCM AES-CMAC AES-CTR AES-ECB AES-XTS
HMAC key	Symmetric key used for message authentication	512 bits - 256 bits	Symmetric key - CSP			HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA3-224 HMAC-SHA3-256 HMAC-SHA3-384 HMAC-SHA3-512

Table 15: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	Input parameter	Hardware register:Plaintext Hardware FIFO:Plaintext	Until module is powered off	Power-off	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
HMAC key	Input parameter	Hardware register:Plaintext Hardware FIFO:Plaintext	Until module is powered off	Power-off	

Table 16: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

N/A for this module.

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 Conditional Self-tests section.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A4289)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption, decryption	Performed during module power-up
AES-ECB (A4289)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption, decryption	Performed during module power-up
AES-CMAC (A4289)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up
HMAC-SHA-1 (A4289)	512 bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up
HMAC-SHA2-256 (A4289)	512 bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up
HMAC-SHA2-512 (A4289)	512 bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up
HMAC-SHA3-512 (A4289)	512 bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up

Table 17: Conditional Self-Tests

Cryptographic algorithm self-tests (CASTs) are automatically performed during power-up of the Qualcomm® Crypto Engine Core without any operator intervention. During CAST execution, no services are available, and input and output are inhibited by the Qualcomm® Crypto Engine Core control logic.

10.3 Periodic Self-Test Information

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM (A4289)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A4289)	KAT	CAST	On demand	Manually by power cycling
AES-CMAC (A4289)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA-1 (A4289)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-256 (A4289)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-512 (A4289)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA3-512 (A4289)	KAT	CAST	On demand	Manually by power cycling

Table 18: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	No cryptographic operation can be performed. No data input or output is possible.	KAT failure	Power cycling	BIST_FAILURE indicator is set

Table 19: Error States

If any of the self-tests fail, the Qualcomm Crypto Engine Core will enter the error state. Data output is prohibited, and no further cryptographic operation is allowed in the error state. 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 module 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.

10.5 Operator Initiation of Self-Tests

The operator can initiate the cryptographic algorithm self-tests by power cycling the module.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Qualcomm® Crypto Engine Core is a sub-chip module that runs on the Snapdragon 8 Gen 3 Mobile 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 like the picture in Figure 2.

If one of these verifications fails, 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 the Self-Tests section will be executed automatically and without operator intervention.

11.2 Administrator 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.

11.3 Non-Administrator Guidance

There is no specific non-Administrator guidance required for the module.

11.4 Design and Rules

N/A Therefore no specific design or rules to be followed.

11.5 Maintenance Requirements

N/A There are no maintenance requirements.

11.6 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.

11.7 Additional Information

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

12.1 Attack List

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