Qualcomm Technologies, Inc.

Qualcomm® Crypto Engine Core

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

Last Update: 2026-07-02

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 versions 5.7.0, 5.7.2, and 5.7.3 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.

This Non-Proprietary Security Policy may be reproduced and distributed, but only whole and intact and including this notice. Other documentation is proprietary to their authors.

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.

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.

[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 crypto services (as listed in Section 4.3) to components residing within the same OE which act as operators. These operators may request services from the modules using FIFOs and registers.
Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

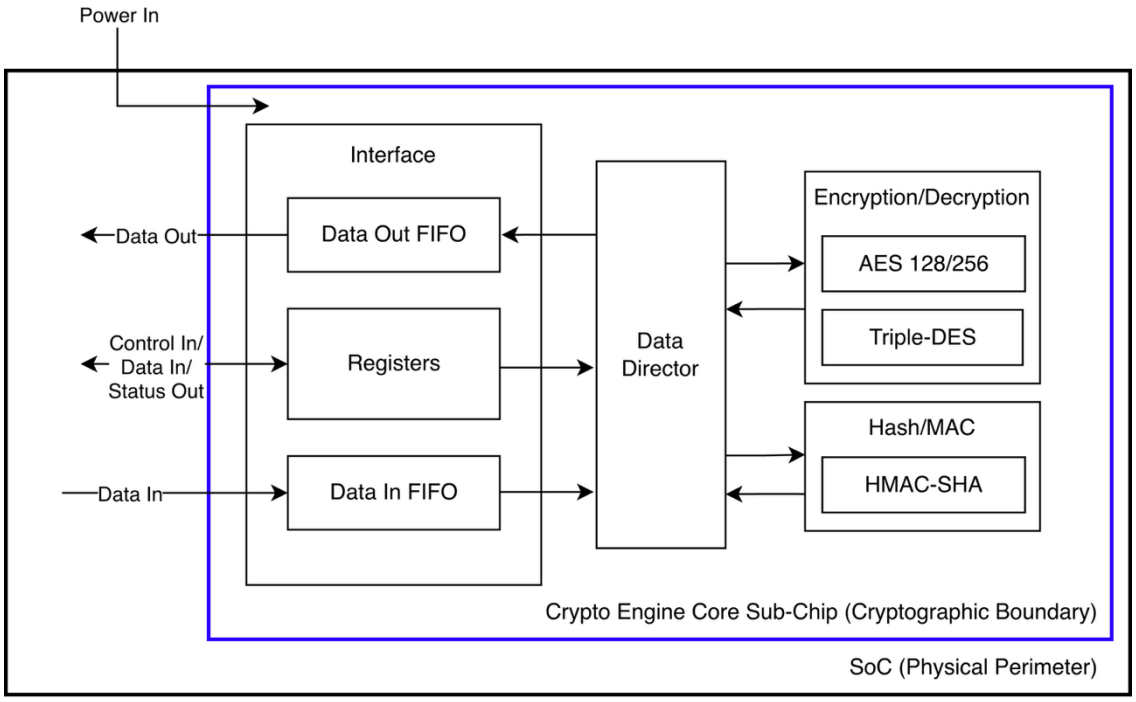

Figure 1: Cryptographic boundary and physical perimeter

Tested Operational Environment's Physical Perimeter (TOEPP):

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

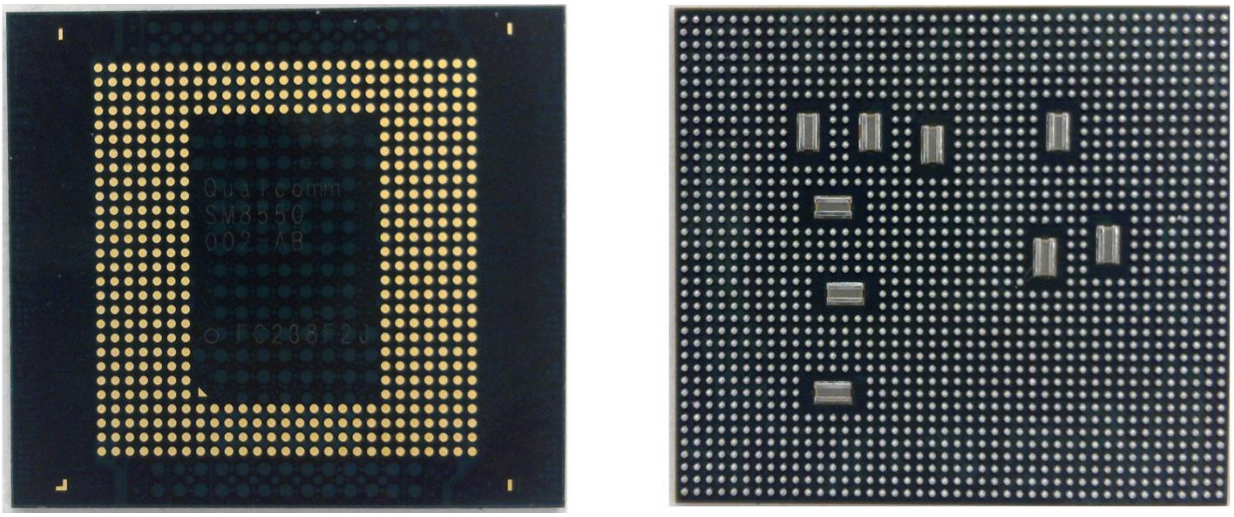

Figure 2: Snapdragon® 8 Gen 2 Mobile Platform

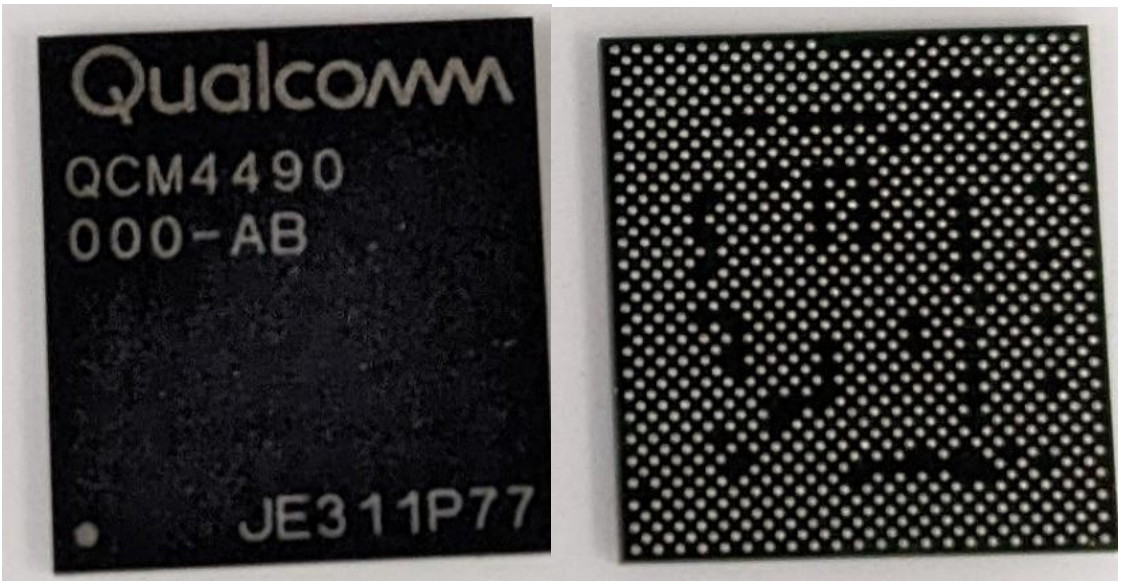

Figure 3 - Qualcomm QCM4490

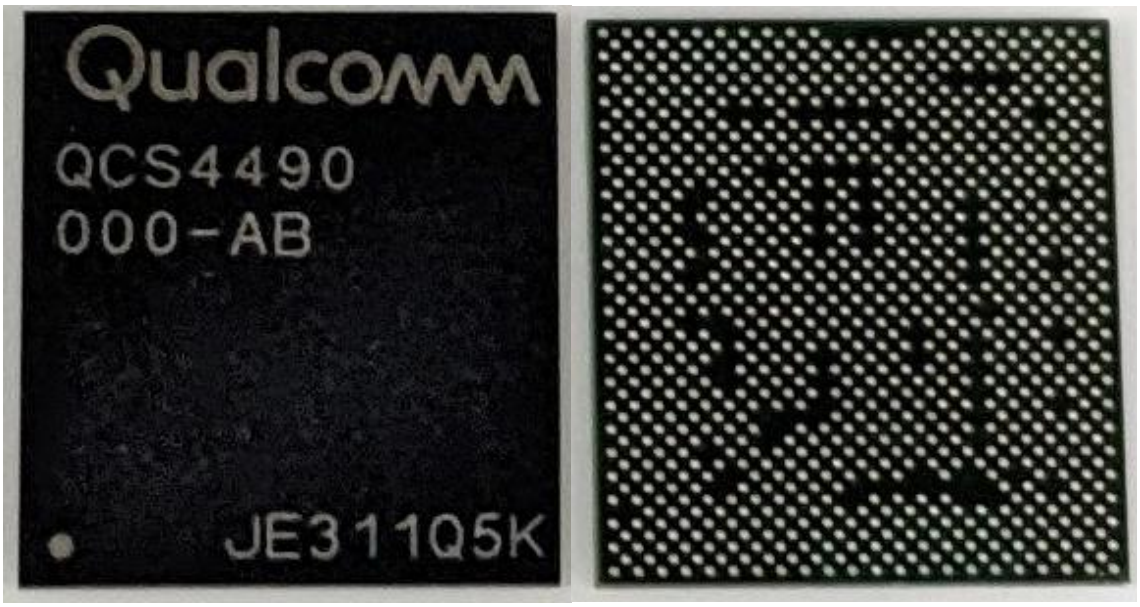

Figure 4 - Qualcomm QCS4490

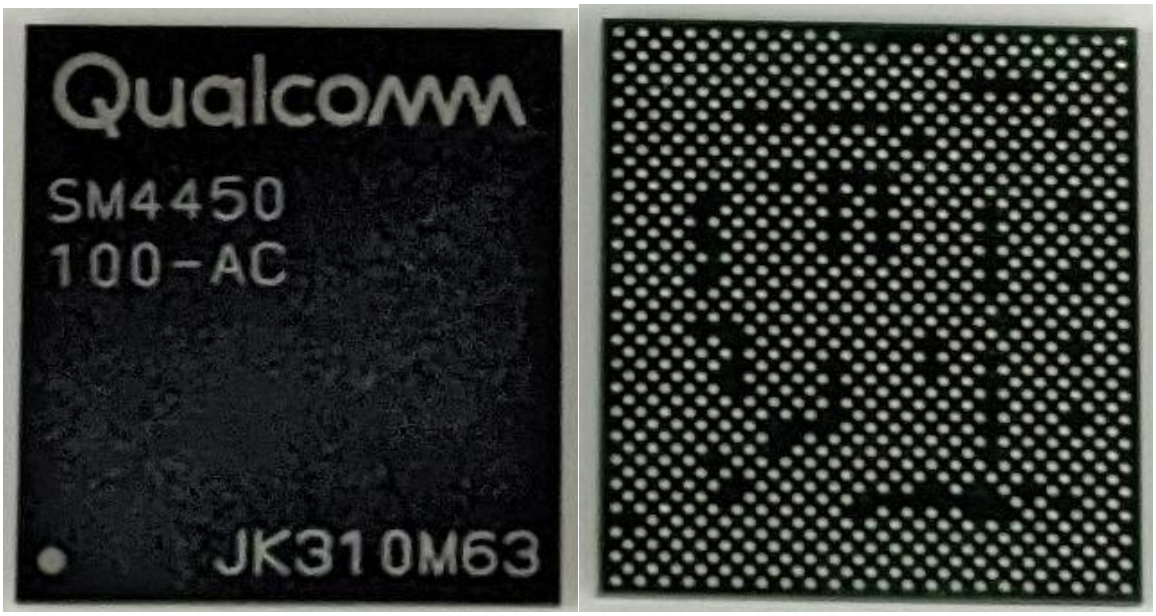

Figure 5 – Snapdragon 4 Gen 2 Mobile Platform

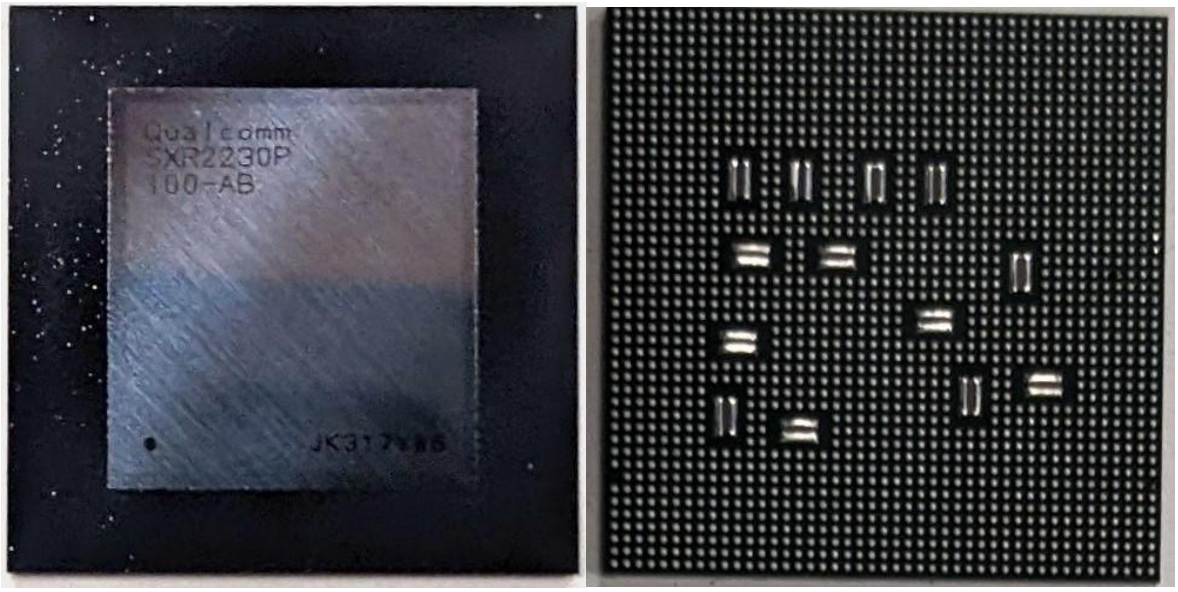

Figure 6 – Snapdragon XR2 Gen 2 Platform

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 2 Mobile Platform	5.7.0	N/A	N/A	N/A
Qualcomm QCM4490	5.7.3	N/A	N/A	N/A
Qualcomm QCS4490	5.7.3	N/A	N/A	N/A
Snapdragon 4 Gen 2 Mobile Platform	5.7.3	N/A	N/A	N/A
Snapdragon XR2 Gen 2 Platform	5.7.2	N/A	N/A	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	Corresponding bit in CRYPTO0_CRYPTO_STATUS4 register is set to 0
Non-approved	Automatically entered whenever a non-	Non-Approved	Non-approved services are not explicitly indicated. The absence of an explicit indicator is an implicit indicator of non-approved services.

Mode Name	Description	Type	Status Indicator
mode of operation	approved service is requested		

Table 3: Modes List and Description

The Qualcomm Crypto Engine Core supports two modes of operation: an approved mode and a non-approved mode.

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	A2908	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CBC	A3694	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CBC	A4464	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CCM	A2908	Key Length - 128, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0, 256 AAD Length - AAD Length: 256, 65536	SP 800-38C
AES-CCM	A3694	Key Length - 128, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0, 256 AAD Length - AAD Length: 256	SP 800-38C
AES-CCM	A4464	Key Length - 128, 256 Tag Length - 112, 128, 32, 48, 64, 80, 96 IV Length - IV Length: 56, 64, 72, 80, 88, 96, 104 Payload Length - Payload Length: 0, 256 AAD Length - AAD Length: 256	SP 800-38C
AES-CMAC	A2908	Direction - Generation, Verification Key Length - 128, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 8-524288 Increment 8	SP 800-38B

Algorithm	CAVP Cert	Properties	Reference
AES-CMAC	A3694	Direction - Generation, Verification Key Length - 128, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 8-524288 Increment 8	SP 800-38B
AES-CMAC	A4464	Direction - Generation, Verification Key Length - 128, 256 MAC Length - MAC Length: 128 Message Length - Message Length: 8-524288 Increment 8	SP 800-38B
AES-CTR	A2908	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - Yes Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A3694	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A4464	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128 Supports Counter larger than maximum value - Yes Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-ECB	A2908	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A3694	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A4464	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A2908	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A3694	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128	SP 800-38E

Algorithm	CAVP Cert	Properties	Reference
		Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	
AES-XTS Testing Revision 2.0	A4464	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 128 Tweak Mode - Hex Data Unit Length Matches Payload Length - Yes	SP 800-38E
HMAC-SHA-1	A2908	MAC - MAC: 160 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA-1	A3694	MAC - MAC: 160 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA-1	A4464	MAC - MAC: 160 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-256	A2908	MAC - MAC: 256 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-256	A3694	MAC - MAC: 256 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-256	A4464	MAC - MAC: 256 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-384	A2908	MAC - MAC: 384 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-384	A3694	MAC - MAC: 384 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-384	A4464	MAC - MAC: 384 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-512	A2908	MAC - MAC: 512 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-512	A3694	MAC - MAC: 512 Key Length - Key Length: 512	FIPS 198-1
HMAC-SHA2-512	A4464	MAC - MAC: 512 Key Length - Key Length: 512	FIPS 198-1
SHA-1	A2908	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA-1	A3694	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA-1	A4464	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A2908	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A3694	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4464	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A2908	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
SHA2-384	A3694	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4464	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A2908	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A3694	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4464	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4

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
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)

Name	Use and Function
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		AES-CBC: (A2908, A3694, A4464)
AES-CCM	BC-Auth	AES in CCM mode		AES-CCM: (A2908, A3694, A4464)
AES-CMAC	MAC	AES in CMAC mode		AES-CMAC: (A2908, A3694, A4464)
AES-CTR	BC-UnAuth	AES in CTR mode		AES-CTR: (A2908, A3694, A4464)
AES-ECB	BC-UnAuth	AES in ECB mode		AES-ECB: (A2908, A3694, A4464)
AES-XTS	BC-UnAuth	AES in XTS mode		AES-XTS Testing Revision 2.0: (A2908, A3694, A4464)
HMAC-SHA-1	MAC	HMAC with SHA-1		HMAC-SHA-1: (A2908, A3694, A4464)
HMAC-SHA2-256	MAC	HMAC with SHA2-256		HMAC-SHA2-256: (A2908, A3694, A4464)
HMAC-SHA2-384	MAC	HMAC with SHA2-384		HMAC-SHA2-384: (A2908, A3694, A4464)
HMAC-SHA2-512	MAC	HMAC with SHA2-512		HMAC-SHA2-512: (A2908, A3694, A4464)
SHA-1	SHA	SHA-1		SHA-1: (A2908, A3694, A4464)
SHA2-256	SHA	SHA2-256		SHA2-256: (A2908, A3694, A4464)
SHA2-384	SHA	SHA2-384		SHA2-384: (A2908, A3694, A4464)
SHA2-512	SHA	SHA2-512		SHA2-512: (A2908, A3694, A4464)

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.

The two AES keys shall be generated and/or established independently according to the rules for component symmetric keys from SP 800-133 Rev. 2, Section 6.3.

2.8 RBG and Entropy

N/A for this module.

2.9 Key Generation

The module does not provide any key generation services.

2.10 Key Establishment

The module does not provide any key establishment services.

2.11 Industry Protocols

The module does not implement any industry protocols, or provide services designed to be used as part of any industry protocol.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
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	N/A

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES Encryption	Perform data encryption	CRYPTO0_CRYPTO_STATUS4 bits 16 and 18 set to 0	AES Key, Plaintext	Ciphertext, Success/Fail	AES-CBC AES-CTR AES-ECB AES-XTS	Crypto Officer - AES key: W,E
AES Decryption	Perform data decryption	CRYPTO0_CRYPTO_STATUS4 bits 16 and 18 set to 0	AES Key, Ciphertext	Plaintext, Success/Fail	AES-CBC AES-CTR AES-ECB AES-XTS	Crypto Officer - AES key: W,E
AES Authenticated Encryption	Perform data encryption	CRYPTO0_CRYPTO_STATUS4 bit 17 set to 0	AES key, plaintext, IV	Ciphertext, tag, Success/Fail	AES-CCM	Crypto Officer - AES key: W,E
AES Authenticated Decryption	Perform data decryption	CRYPTO0_CRYPTO_STATUS4 bit 17 set to 0	AES key, ciphert	Plaintext, Success/Fail	AES-CCM	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			ext, tag, IV			- 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	Crypto Officer - HMAC key: W,E
Hash	Hashing	CRYPTO0_CRYPTO_STATUS4 bits 21-24 set to 0	Input data	Hash output	SHA-1 SHA2-256 SHA2-384 SHA2-512	Crypto Officer
Show Status	Return the module status	None	N/A	Module status	None	Crypto Officer
Self-Test	Self-Tests are executed automatically when device is	None	None	Self-test Success/Fail	AES-CBC AES-CCM AES-CMAC	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	booted or restarted				AES-CTR AES-ECB AES-XTS HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 SHA-1 SHA2-256 SHA2-384 SHA2-512	
Zeroization	Zeroizes all SSPs	None	None	None	None	Crypto Officer - AES key: Z - HMAC key: Z
Show version	Show the version and name	None	None	Name and version information read from register	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	of the module			CRYPTO0_CRYPTO_VERSION		

Table 9: Approved Services

G = **Generate**: The module generates or derives the SSP.
E = Execute: The module uses the SSP in performing a cryptographic operation.
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.
Z = **Zeroize**: The module zeroizes the SSP.

4.4 Non-Approved Services

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

How Requirements are Satisfied:

N/A for this module.

6.2 Configuration Settings and Restrictions

N/A for this module.

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 is a sub-chip enclosed in the platforms that are listed in Table 2 that are made up of production grade component and conform to the Level 2 requirements for physical security.

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

The Qualcomm Crypto Engine Core is further protected by being enclosed in commercial off the shelf mobile device utilizing production grade commercially available components and that the mobile device enclosure that 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 only stores SSPs for the duration of service execution. 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 output services. 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.

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

A successful power-off indicates that all SSPs have been zeroized. Data output is inhibited during this zeroization process.

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-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						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

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	
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-CBC (A2908) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CBC (A2908) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CBC (A3694) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CBC (A3694) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CBC (A4464) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CBC (A4464) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CCM (A2908) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CCM (A2908) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CCM (A3694) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CCM (A3694) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CCM (A4464) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CCM (A4464) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-ECB (A2908) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A2908) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-ECB (A3694) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A3694) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-ECB (A4464) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A4464) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CTR (A2908) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CTR (A2908) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CTR (A3694) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CTR (A3694) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CTR (A4464) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CTR (A4464) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-XTS Testing Revision 2.0 (A2908) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-XTS Testing Revision 2.0 (A2908) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-XTS Testing Revision 2.0 (A3694) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-XTS Testing Revision 2.0 (A3694) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-XTS Testing Revision 2.0 (A4464) - Encryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-XTS Testing Revision 2.0 (A4464) - Decryption	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CMAC (A2908)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CMAC (A3694)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up
AES-CMAC (A4464)	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 (A2908)	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-SHA-1 (A3694)	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-SHA-1 (A4464)	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 (A2908)	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 (A3694)	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 (A4464)	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-SHA2-384 (A2908)	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-SHA2-384 (A3694)	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-SHA2-384 (A4464)	512 bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC-SHA2-512 (A2908)	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 (A3694)	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 (A4464)	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. If any CAST fails, the module will enter the error state.

10.3 Periodic Self-Test Information

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A2908) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CBC (A2908) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CBC (A3694) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CBC (A3694) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CBC (A4464) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CBC (A4464) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CCM (A2908) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CCM (A2908) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CCM (A3694) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CCM (A3694) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CCM (A4464) - Encryption	KAT	CAST	On demand	Manually by power cycling

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM (A4464) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A2908) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A2908) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A3694) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A3694) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A4464) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A4464) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CTR (A2908) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CTR (A2908) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CTR (A3694) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CTR (A3694) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CTR (A4464) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CTR (A4464) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-XTS Testing Revision 2.0 (A2908) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-XTS Testing Revision 2.0 (A2908) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-XTS Testing Revision 2.0 (A3694) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-XTS Testing Revision 2.0 (A3694) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-XTS Testing Revision 2.0 (A4464) - Encryption	KAT	CAST	On demand	Manually by power cycling

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-XTS Testing Revision 2.0 (A4464) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CMAC (A2908)	KAT	CAST	On demand	Manually by power cycling
AES-CMAC (A3694)	KAT	CAST	On demand	Manually by power cycling
AES-CMAC (A4464)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA-1 (A2908)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA-1 (A3694)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA-1 (A4464)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-256 (A2908)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-256 (A3694)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-256 (A4464)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-384 (A2908)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-384 (A3694)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-384 (A4464)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-512 (A2908)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-512 (A3694)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-512 (A4464)	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

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 and inhibiting data output 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 chips listed in Table 2.

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 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.

12 Mitigation of Other Attacks

12.1 Attack List

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 Encryption Standard
ECB	Electronic Code Book
FIFO	First-in First-out (Queue)
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PCB	Printed Circuit Board
SHA	Secure Hash Algorithm
SoC	System on a Chip
SSP	Sensitive Security Parameter
TDES	Triple-DES
TOEPP	Tested Operational 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
SP800-140Br1	**NIST Special Publication 800-140B Revision 1 - CMVP Security Policy Requirements** November 2023 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140Br1.pdf