

Qualcomm Technologies, Inc.

Qualcomm® Crypto Engine Core

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

Last Update: 2026-11-18

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

https://www.atsec.com

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Table of Contents

1 General 5
1.1 Overview 5
1.2 Security Levels 5
1.3 Additional Information 5
2 Cryptographic Module Specification 7
2.1 Description 7
2.2 Tested and Vendor Affirmed Module Version and Identification 8
2.3 Excluded Components 8
2.4 Modes of Operation 8
2.5 Algorithms 9
2.6 Security Function Implementations 11
2.7 Algorithm Specific Information 13
2.7.1 AES XTS 13
2.7.2 Use of TDES 13
2.7.3 Use of SHA-1 and SHA3-224 13
2.8 RBG and Entropy 13
2.9 Key Generation 13
2.10 Key Establishment 13
2.11 Industry Protocols 13
3 Cryptographic Module Interfaces 14
3.1 Ports and Interfaces 14
4 Roles, Services, and Authentication 15
4.1 Authentication Methods 15
4.2 Roles 15
4.3 Approved Services 16
4.4 Non-Approved Services 21
4.5 External Software/Firmware Loaded 21
5 Software/Firmware Security 22
5.1 Integrity Techniques 22
6 Operational Environment 23
6.1 Operational Environment Type and Requirements 23
6.2 Configuration Settings and Restrictions 23
7 Physical Security 24
7.1 Mechanisms and Actions Required 24

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

8 Non-Invasive Security 25
8.1 Mitigation Techniques 25
9 Sensitive Security Parameters Management 26
9.1 Storage Areas 26
9.2 SSP Input-Output Methods 26
9.3 SSP Zeroization Methods 26
9.4 SSPs 26
9.5 Transitions 28
10 Self-Tests 29
10.1 Pre-Operational Self-Tests 29
10.2 Conditional Self-Tests 29
10.3 Periodic Self-Test Information 32
10.4 Error States 33
10.5 Operator Initiation of Self-Tests 33
11 Life-Cycle Assurance 34
11.1 Installation, Initialization, and Startup Procedures 34
11.2 Administrator Guidance 34
11.3 Non-Administrator Guidance 34
11.4 End of Life 34
12 Mitigation of Other Attacks 35
12.1 Attack List 35
Appendix A: Glossary and Abbreviations 36
Appendix B: References 37

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

List of Tables

Table 1: Security Levels 5
Table 2: Tested Module Identification – Hardware 8
Table 3: Modes List and Description 9
Table 4: Approved Algorithms 10
Table 5: Non-Approved, Not Allowed Algorithms 11
Table 6: Security Function Implementations 13
Table 7: Ports and Interfaces 14
Table 8: Roles 15
Table 9: Approved Services 20
Table 10: Non-Approved Services 21
Table 11: Mechanisms and Actions Required 24
Table 12: Storage Areas 26
Table 13: SSP Input-Output Methods 26
Table 14: SSP Zeroization Methods 26
Table 15: SSP Table 1 27
Table 16: SSP Table 2 28
Table 17: Conditional Self-Tests 31
Table 18: Conditional Periodic Information 33
Table 19: Error States 33

List of Figures

Figure 1: Cryptographic boundary and physical perimeter 7
Figure 2: Snapdragon® 8 Gen 5 Mobile Platform 8
Figure 3: Snapdragon® 8 Elite Gen 5 Mobile Platform 8

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

1 General

1.1 Overview

This Security Policy describes the features and design of version 6.0.0 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

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

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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 version 6.0.0 of the Qualcomm Crypto Engine Core. It has a one-to-one mapping to 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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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 module using FIFOs and registers.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

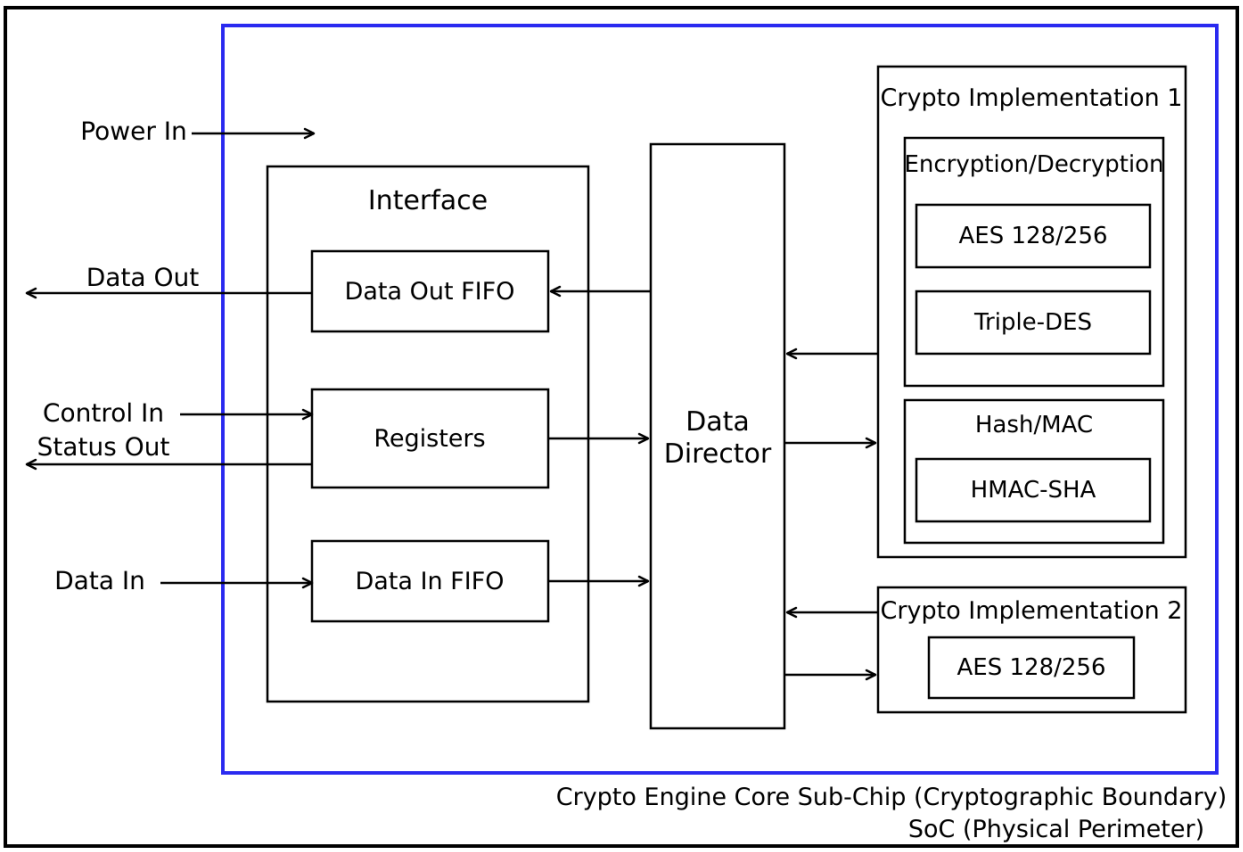


Figure 1: Cryptographic boundary and physical perimeter

Tested Operational Environment's Physical Perimeter (TOEPP):

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

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

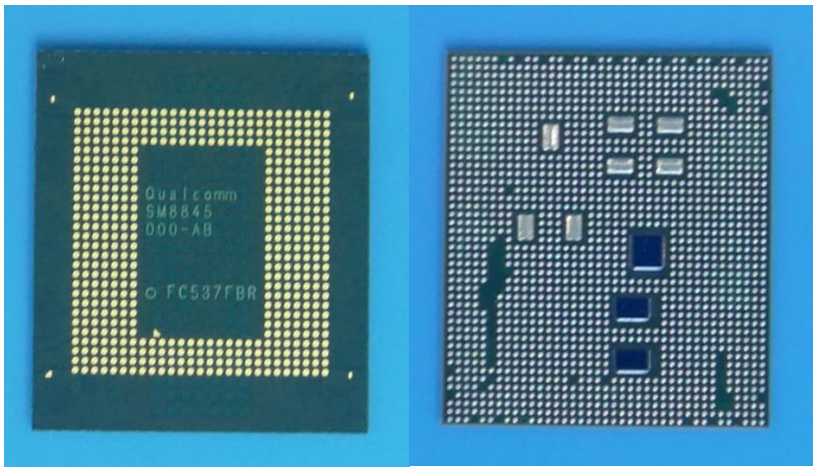


Figure 2: Snapdragon® 8 Gen 5 Mobile Platform

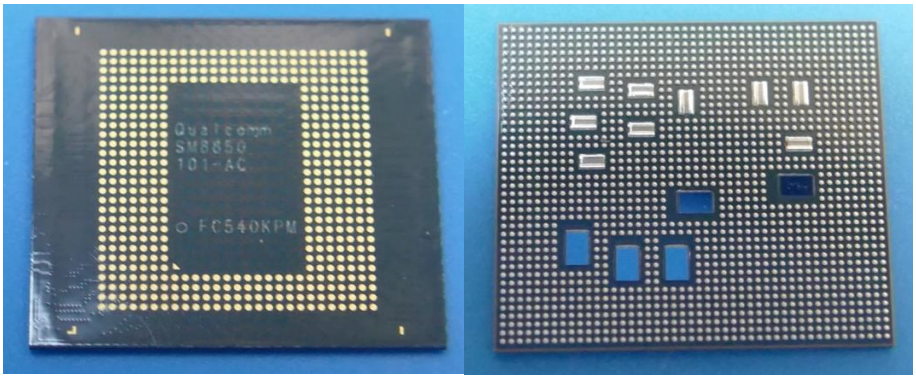


Figure 3: Snapdragon® 8 Elite Gen 5 Mobile Platform

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 5 Mobile Platform	6.0.0	N/A	N/A	N/A
Snapdragon 8 Elite Gen 5 Mobile Platform	6.0.0	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:

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Mode Name	Description	Type	Status Indicator
Approved mode of operation	Automatically entered whenever an approved service is requested	Approved	Corresponding bit in CRYPTO0_CRYPTO_FIPS_APPROVED is set to 0
Non-approved mode of operation	Automatically entered whenever a non-approved service is requested	Non-Approved	Non-approved services are not explicitly indicated.

Table 3: Modes List and Description

The Qualcomm Crypto Engine Core supports two modes of operation: approved mode and 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	A7988, A7989	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CBC-CS2	A7988, A7989	Direction - decrypt, encrypt Key Length - 128, 256	SP 800-38A
AES-CCM	A7988	Key Length - 128, 256	SP 800-38C
AES-CMAC	A7988	Direction - Generation Key Length - 128, 256	SP 800-38B
AES-CTR	A7988, A7989	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A7988, A7989	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A7988	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38E
HMAC-SHA-1	A7988	Key Length - Key Length: 128, 224, 256, 384, 448, 512	FIPS 198-1
HMAC-SHA2-256	A7988	Key Length - Key Length: 128, 224, 256, 384, 448, 512	FIPS 198-1
HMAC-SHA2-384	A7988	Key Length - Key Length: 128, 224, 256, 384, 448, 512	FIPS 198-1

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-512	A7988	Key Length - Key Length: 128, 224, 256, 384, 448, 512	FIPS 198-1
HMAC-SHA3-224	A7988	Key Length - Key Length: 128, 224, 256, 384, 448, 512	FIPS 198-1
HMAC-SHA3-256	A7988	Key Length - Key Length: 128, 224, 256, 384, 448, 512	FIPS 198-1
HMAC-SHA3-384	A7988	Key Length - Key Length: 128, 224, 256, 384, 448, 512	FIPS 198-1
HMAC-SHA3-512	A7988	Key Length - Key Length: 128, 224, 256, 384, 448, 512	FIPS 198-1
SHA-1	A7988	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A7988	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-384	A7988	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A7988	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-224	A7988	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-256	A7988	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-384	A7988	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHA3-512	A7988	Message Length - Message Length: 0-65536 Increment 8	FIPS 202
SHAKE-128	A7988	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
SHAKE-256	A7988	Output Length - Output Length: 16-65536 Increment 8	FIPS 202
TDES-CBC	A7988	Direction - Decrypt, Encrypt	SP 800-67 Rev. 2
TDES-ECB	A7988	Direction - Decrypt, Encrypt	SP 800-67 Rev. 2

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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 (non-approved due to non-compliance with IV requirements)
AES-SIV	encryption, decryption
DES-CBC	encryption, decryption
DES-ECB	encryption, decryption
TDES (two independent keys)	encryption, decryption
TDES Encryption (three independent keys)	encryption
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
cSHAKE	extendable output function (non-approved due to no CAVP certificate)
KMAC	message authentication code (non-approved due to no CAVP certificate)

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: (A7988, A7989)
AES-CCM	BC-Auth	AES in CCM mode		AES-CCM: (A7988)
AES-CTR	BC-UnAuth	AES in CTR mode		AES-CTR: (A7988, A7989)
AES-ECB	BC-UnAuth	AES in ECB mode		AES-ECB: (A7988, A7989)

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Type	Description	Properties	Algorithms
AES-CBC-CS2	BC-UnAuth	AES in CBC-CS2 mode		AES-CBC-CS2: (A7988, A7989)
AES-XTS	BC-UnAuth	AES in XTS mode		AES-XTS Testing Revision 2.0: (A7988)
AES-CMAC	MAC	AES in CMAC mode		AES-CMAC: (A7988)
TDES-ECB (Legacy Use)	BC-UnAuthDecrypt	TDES-ECB with three independent keys	Direction:Decryption	TDES-ECB: (A7988)
TDES-CBC (Legacy Use)	BC-UnAuthDecrypt	TDES-CBC with three independent keys	Direction:Decryption	TDES-CBC: (A7988)
HMAC-SHA-1	MAC	HMAC with SHA-1		HMAC-SHA-1: (A7988)
HMAC-SHA2-256	MAC	HMAC with SHA2-256		HMAC-SHA2-256: (A7988)
HMAC-SHA2-384	MAC	HMAC with SHA2-384		HMAC-SHA2-384: (A7988)
HMAC-SHA2-512	MAC	HMAC with SHA2-512		HMAC-SHA2-512: (A7988)
HMAC-SHA3-224	MAC	HMAC with SHA3-224		HMAC-SHA3-224: (A7988)
HMAC-SHA3-256	MAC	HMAC with SHA3-256		HMAC-SHA3-256: (A7988)
HMAC-SHA3-384	MAC	HMAC with SHA3-384		HMAC-SHA3-384: (A7988)
HMAC-SHA3-512	MAC	HMAC with SHA3-512		HMAC-SHA3-512: (A7988)
SHA-1	SHA	SHA-1		SHA-1: (A7988)
SHA2-256	SHA	SHA2-256		SHA2-256: (A7988)
SHA2-384	SHA	SHA2-384		SHA2-384: (A7988)
SHA2-512	SHA	SHA2-512		SHA2-512: (A7988)
SHA3-224	SHA	SHA3-224		SHA3-224: (A7988)
SHA3-256	SHA	SHA3-256		SHA3-256: (A7988)
SHA3-384	SHA	SHA3-384		SHA3-384: (A7988)
SHA3-512	SHA	SHA3-512		SHA3-512: (A7988)

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Type	Description	Properties	Algorithms
SHAKE-128	XOF	SHAKE-128		SHAKE-128: (A7988)
SHAKE-256	XOF	SHAKE-256		SHAKE-256: (A7988)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES XTS

AES-XTS is only approved for storage purposes. Per IG C.I, AES-XTS Key_1 and/or Key_2, when entered into the module by the operator, shall be generated and/or established independently of each other according to the rules for component symmetric keys from NIST SP 800-133rev2, Sec. 6.3. for an approved use of AES-XTS.

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.

2.7.2 Use of TDES

Three-key TDES decryption is approved only for Legacy Use. Algorithms designated as “Legacy” can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M.

2.7.3 Use of SHA-1 and SHA3-224

The SHA-1 and SHA3-224 algorithms are available “as is” in Approved mode. Their use is approved only for message digests and HMAC-based message authentication. The module does not support any other Approved use of SHA-1 or SHA3-224. Starting in 2031, SHA-1 and SHA3-224 will be approved only for legacy use (i.e. to process data which was cryptographically protected prior to 2031).

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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Data In FIFO and 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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES Encryption	Perform data encryption	CRYPTO0_CRYPTO_FIPS_APPROVED bits 0 and 2 set to 0	AES Key, Plaintext	Ciphertext, Success/Fail	AES-CBC AES-CTR AES-ECB AES-XTS AES-CBC-CS2	Crypto Officer - AES key: W,E
AES Decryption	Perform data decryption	CRYPTO0_CRYPTO_FIPS_APPROVED bits 0 and 2 set to 0	AES Key, Ciphertext	Plaintext, Success/Fail	AES-CBC AES-CTR AES-ECB AES-XTS AES-CBC-CS2	Crypto Officer - AES key: W,E
AES Authenticated Encryption	Perform data encryption	CRYPTO0_CRYPTO_FIPS_APPROVED bit 1 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_FIPS_APPROVED bit 1 set to 0	AES Key, Ciphertext, tag, IV	Plaintext, Success/Fail	AES-CCM	Crypto Officer - AES key: W,E
CMAC Message Authentication	Message Authentication	CRYPTO0_CRYPTO_FIPS_APPROVED bit 13 set to 0	AES Key, Input data	CMAC value	AES-CMAC	Crypto Officer - AES key: W,E

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
TDES Decryption (Legacy Use)	Decrypt data which was encrypted with 3-key TDES prior to the sunset date provided in IG C.M	CRYPTO0_CRYPTO_FIPS_APPROVED bit 3 set to 0	Triple-DES key, ciphertext	Plaintext	TDES-ECB (Legacy Use) TDES-CBC (Legacy Use)	Crypto Officer - Triple-DES Key: W,E
HMAC Message Authentication	Message Authentication	CRYPTO0_CRYPTO_FIPS_APPROVED bits 9-12, 18-21 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-SHA3-512	Crypto Officer - HMAC key: W,E
Hash	Hashing	CRYPTO0_CRYPTO_FIPS_APPROVED bits 5-8, 14-17 set to 0	Input data	Hash output	SHA-1 SHA2-	Crypto Officer

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					256 SHA2-384 SHA2-512 SHA3-224 SHA3-256 SHA3-384 SHA3-512	
XOF	Extendable output function	CRYPTO0_CRYPTO_FIPS_APPROVED bit 22 set to 0	Input data, output length	XOF output	SHAKE-128 SHAKE-256	Crypto Officer
Show Status	Return codes read from CRYPTO0_CRYPTO_BIST_STATUS and CRYPTO0_CFG1_CRYPTO_BIST_STATUS	None	N/A	Both zero (operational) or either non-zero (error)	None	Crypto Officer
Self-Test	Self-Tests are executed automatically when device is booted or restarted	None	None	Self-test Success/Fail	AES-CBC AES-CCM AES-CTR AES-ECB AES-XTS AES-CMAC TDES-ECB (Legacy Use) TDES-	Crypto Officer

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					CBC (Legacy Use) HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA3-256 HMAC-SHA3-512 SHAKE-256	
Zeroization	Zeroizes all SSPs	None	None	None	None	Crypto Officer - AES key: Z - HMAC key: Z - Triple-DES Key: Z

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show identifier and version	Show the module identifier and module version	None	None	Identifier and version information read from registers CRYPTO0_CRYPTO_FIPS_ID and CRYPTO0_CRYPTO_VERSION	None	Crypto Officer

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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Encryption	Encrypts data using symmetric cryptography	AES-GCM AES-SIV DES-CBC DES-ECB TDES (two independent keys) TDES Encryption (three independent keys) SM4	CO
Decryption	Decrypts data using symmetric cryptography	AES-GCM AES-SIV DES-CBC DES-ECB TDES (two independent keys) SM4	CO
Hash	Hashing algorithm	SM3	CO
Message Authentication	Computes the MAC value of data	KMAC	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
Extendable Output Function (XOF)	Extendable Output Function	cSHAKE	CO

Table 10: Non-Approved Services

4.5 External Software/Firmware Loaded

Not Applicable. No external software or firmware is loaded.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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 Section 2.2 that are made up of production grade components 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 that uses production-grade, commercially available components, and whose enclosure completely surrounds the Qualcomm Crypto Engine Core.

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

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

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 operational 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
Reset signal	Explicit zeroization within module	The registers holding the SSPs are set to all zeroes	A component within the SoC may de-assert the module's reset signal to invoke zeroization

Table 14: SSP Zeroization Methods

A successful reset 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-CMAC AES-CTR

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						AES-ECB AES-XTS
HMAC key	Symmetric key used for message authentication	128/192/256/384/448/512 bits - 128/192/256/256/256/256 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
Triple-DES Key	Symmetric key used for legacy data decryption	168 bits - 112 bits	Symmetric key - CSP			TDES-ECB (Legacy Use) TDES-CBC (Legacy Use)

Table 15: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	Input parameter	Registers:Plaintext Hardware FIFO:Plaintext	Until module is reset	Reset signal	
HMAC key	Input parameter	Registers:Plaintext Hardware FIFO:Plaintext	Until module is reset	Reset signal	
Triple-DES Key	Input parameter	Hardware FIFO:Plaintext Registers:Plaintext	Until module is reset	Reset signal	

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Table 16: SSP Table 2

9.5 Transitions

Beginning in 2031,

- cryptographic mechanisms providing less than 128 bit of security strength, shall no longer be used to apply cryptographic protection and are limited to legacy use for processing, as specified in Table 4 of NIST SP 800-57 Part 1 Rev. 5.
- SHA-1 and SHA3-224 will be approved only for legacy use (i.e. to process data which was cryptographically protected prior to 2031).

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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 the Conditional Self-tests section.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A7988) - Encryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A7989) - Encryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A7988) - Decryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-ECB (A7989) - Decryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CTR (A7988) - Encryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CTR (A7989) - Encryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CTR (A7988) - Decryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CTR (A7989) - Decryption	256-bit key	KAT	CAST	Module becomes operational and	Decryption	Performed during module power-up

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
AES-CBC (A7988) - Encryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CBC (A7989) - Encryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CBC (A7988) - Decryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CBC (A7989) - 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 (A7988) - 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 (A7988) - Decryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CCM (A7988) - Encryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-CCM (A7988) - Decryption	256-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-CMAC (A7988)	256-bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up
TDES-ECB (A7988)	168-bit key	KAT	CAST	Module becomes operational and	Decryption (Legacy)	Performed during module power-up

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				services are available for use		
TDES-CBC (A7988)	168-bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption (Legacy)	Performed during module power-up
HMAC-SHA-1 (A7988)	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 (A7988)	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 (A7988)	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 (A7988)	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 (A7988)	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-SHA3-256 (A7988)	512-bit key	KAT	CAST	Module becomes operational and services are available for use	MAC tag computation and verification	Performed during module power-up
SHAKE-256 (A7988)	N/A	KAT	CAST	Module becomes operational and services are available for use	XOF	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 data input and output are inhibited by the Qualcomm Crypto Engine Core control logic. If any CAST fails, the module will enter the error state.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

10.3 Periodic Self-Test Information

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A7988) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A7989) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A7988) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A7989) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CTR (A7988) - Encryption	KAT	CAST	On Demand	Manually by power cycling
AES-CTR (A7989) - Encryption	KAT	CAST	On Demand	Manually by power cycling
AES-CTR (A7988) - Decryption	KAT	CAST	On Demand	Manually by power cycling
AES-CTR (A7989) - Decryption	KAT	CAST	On Demand	Manually by power cycling
AES-CBC (A7988) - Encryption	KAT	CAST	On Demand	Manually by power cycling
AES-CBC (A7989) - Encryption	KAT	CAST	On Demand	Manually by power cycling
AES-CBC (A7988) - Decryption	KAT	CAST	On Demand	Manually by power cycling
AES-CBC (A7989) - Decryption	KAT	CAST	On Demand	Manually by power cycling
AES-XTS Testing Revision 2.0 (A7988) - Encryption	KAT	CAST	On Demand	Manually by power cycling
AES-XTS Testing Revision 2.0 (A7988) - Decryption	KAT	CAST	On Demand	Manually by power cycling
AES-CCM (A7988) - Encryption	KAT	CAST	On demand	Manually by power cycling
AES-CCM (A7988) - Decryption	KAT	CAST	On demand	Manually by power cycling
AES-CMAC (A7988)	KAT	CAST	On demand	Manually by power cycling

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
TDES-ECB (A7988)	KAT	CAST	On Demand	Manually by power cycling
TDES-CBC (A7988)	KAT	CAST	On Demand	Manually by power cycling
HMAC-SHA-1 (A7988)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-256 (A7988)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-512 (A7988)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA2-384 (A7988)	KAT	CAST	On Demand	Manually by power cycling
HMAC-SHA3-512 (A7988)	KAT	CAST	On demand	Manually by power cycling
HMAC-SHA3-256 (A7988)	KAT	CAST	On Demand	Manually by power cycling
SHAKE-256 (A7988)	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	At least one of the registers CRYPTO0_CRYPTO_BIST_STATUS or CRYPTO0_CFG1_CRYPTO_BIST_STATUS are non-zero

Table 19: Error States

While in the error state, all data input and output is 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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

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 Section 2.2.

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 either Figure 2 or Figure 3 depending on the SoC model.

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

To verify the module's name and version, an administrator may invoke the module's "Show identifier and version" service by checking the CRYPTO0_CRYPTO_FIPS_ID and CRYPTO0_CRYPTO_VERSION registers. The CRYPTO0_CRYPTO_FIPS_ID register must hold the value 0x00000001, which identifies the module as the Qualcomm Crypto Engine Core. The CRYPTO0_CRYPTO_VERSION register must hold the value 0x06000000, representing the module version 6.0.0.

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.

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.

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

12 Mitigation of Other Attacks

12.1 Attack List

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

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Appendix A: Glossary and Abbreviations

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cybersecurity
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DES	Data Encryption Standard
FIFO	First In, First Out
FIPS	Federal Information Processing Standards Publication
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
OTP	One-Time Programmable
SHA	Secure Hash Algorithm
SoC	System on a Chip
XTS	XEX Tweakable Block Cipher with Ciphertext Stealing

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.

Appendix B: References

FIPS 140-3	**FIPS PUB 140-3 - Security Requirements For Cryptographic Modules** March 2019 https://doi.org/10.6028/NIST.FIPS.140-3
FIPS 140-3 IG	**Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program** February 2026 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements
FIPS 197	**Advanced Encryption Standard (AES)** May 2023 https://doi.org/10.6028/NIST.FIPS.197-upd1
SP 800-38A	**Recommendation for Block Cipher Modes of Operation Methods and Techniques** December 2001 https://doi.org/10.6028/NIST.SP.800-38A
SP 800-38B	**Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication** May 2005 https://doi.org/10.6028/NIST.SP.800-38B
SP 800-38C	**Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality** May 2004 https://doi.org/10.6028/NIST.SP.800-38C
SP 800-38E	**Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality of Storage Devices** January 2010 https://doi.org/10.6028/NIST.SP.800-38E
SP 800-67r2	**Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher** November 2017 https://doi.org/10.6028/NIST.SP.800-67r2
FIPS 180-4	**Secure Hash Standard (SHS)** August 2015 https://doi.org/10.6028/NIST.FIPS.180-4
FIPS 202	**SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions** August 2015 https://doi.org/10.6028/NIST.FIPS.202
FIPS 198-1	**The Keyed-Hash Message Authentication Code (HMAC)** July 2008 https://doi.org/10.6028/NIST.FIPS.198-1

© 2026 Qualcomm Technologies, Inc. and/or its affiliated companies. All rights reserved.