Qualcomm Technologies, Inc.

Qualcomm® Crypto Engine Core

Version 5.6.0

FIPS 140-2 Non-Proprietary Security Policy

Version: 1.4

2023-10-30

Prepared for:

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121

Prepared by:

atsec information security Corp.
9130 Jollyville Road, Suite 260
Austin, TX 78759

TABLE OF CONTENTS

1. Introduction

This document is a FIPS 140-2 Security Policy for the Qualcomm Crypto Engine Core cryptographic module. The version number of the Qualcomm Crypto Engine Core is 5.6.0. This document contains a specification of the rules under which the Qualcomm Crypto Engine Core must operate. It also describes how this Qualcomm Crypto Engine Core meets the requirements as specified in Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2) for a Security Level 2 module. It is intended for the FIPS 140-2 testing lab, Cryptographic Module Validation Program (CMVP), developers working on the release, administrators and users of the Qualcomm Crypto Engine Core.

For more information about the FIPS 140-2 standard and validation program, refer to the NIST website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

1.1.Purpose of the Security Policy

There are three major reasons that a security policy is required:

- It is required for FIPS 140-2 validation.
- It allows individuals and organizations to determine whether the implemented Qualcomm Crypto Engine Core satisfies the stated security policy.
- It allows individuals and organizations to determine whether the described capabilities, level of protection, and access rights provided by the Qualcomm Crypto Engine Core meet their security requirements.

2. Cryptographic Module Specification

2.1.Module description

The Qualcomm Crypto Engine Core is a single-chip hardware module implemented as a sub-chip in the Qualcomm® Snapdragon™ 888 5G Mobile Platform SoC, Qualcomm® QCM6490 SoC, Qualcomm® QCS6490 SoC, and Qualcomm® Snapdragon™ 695 5G Mobile Platform SoC. From the validation perspective, the Qualcomm Crypto Engine Core is configured as a single chip hardware module. The cryptographic services provided by the Qualcomm Crypto Engine Core are:

- Data encryption / decryption utilizing symmetric ciphers, i.e., Triple-DES, and AES algorithms.
- Computation of hash values, i.e., SHA-1, SHA-256, SHA-384 and SHA-512.
- Message authentication utilizing HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512, AES CMAC, hashing algorithms.
- Hashing and ciphering operations using AES CCM.

Please refer to Table 4-2 for the algorithm certificates of the FIPS approved algorithms listed below.

Table 2-1: Summary of FIPS approved and FIPS non-approved algorithms in the Qualcomm Crypto Engine Core

FIPS Approved	Implemented Algorithms
AES-128 CBC, AES-256 CBC	encryption, decryption
AES-128 ECB, AES-256 ECB	encryption, decryption
AES-128 CTR, AES-256 CTR	encryption, decryption
AES-128 XTS, AES-256 XTS	encryption, decryption
AES-128 CCM, AES-256 CCM	encryption, decryption (with message authentication code)
Triple-DES CBC (three-key)	encryption, decryption
Triple-DES ECB (three-key)	encryption, decryption
SHA-1	hashing
SHA-256	hashing
SHA-384	hashing
SHA-512	hashing
HMAC SHA-1 with key sizes between 112 bits and 512 bits	message authentication code
HMAC SHA-256 with key sizes between 112 bits and 512 bits	message authentication code
HMAC SHA-384 with key sizes between 112 bits and 512 bits	message authentication code
HMAC SHA-512 with key sizes between 112 bits and 512 bits	message authentication code
AES-128-CMAC AES-256-CMAC	message authentication code
Non-Approved	**Implemented Algorithms**
AES-GCM	encryption, decryption

DES CBC	encryption, decryption
DES ECB	encryption, decryption
Triple-DES (two-key)	encryption, decryption
HMAC SHA-1 with key sizes below 112 bits	message authentication code
HMAC SHA-256 with key sizes below 112 bits	message authentication code
HMAC SHA-384 with key sizes below 112 bits	message authentication code
HMAC SHA-512 with key sizes below 112 bits	message authentication code
AEAD-SHA-1 AES CBC	encryption, decryption (with message authentication code)
AEAD-SHA-1 AES CTR	encryption, decryption (with message authentication code)
AEAD-SHA-1 DES CBC	encryption, decryption (with message authentication code)
AEAD-SHA-1 Triple-DES CBC	encryption, decryption (with message authentication code)

2.1.1.Hardware Description

The Qualcomm Crypto Engine Core is implemented in the Qualcomm Crypto Engine Core 5.6.0 hardware, which resides in the Snapdragon 888 5G Mobile Platform, Qualcomm QCM6490, Qualcomm QCS6490, and Qualcomm Snapdragon 695 5G Mobile Platform SoCs. The Qualcomm Crypto Engine Core 5.6.0 provide a series of algorithms (as listed in Table 2-1) implemented in the device hardware.

2.1.2.Module Validation Level

The Qualcomm Crypto Engine Core is intended to meet requirements of FIPS 140-2 at an overall Security Level 2. The following table shows the security level claimed for each of the eleven sections that comprise the validation:

Table 2-2: Security Levels

FIPS 140-2 Sections	Security Level				
	N/A	1	2	3	4
Cryptographic Module Specification			X		
Cryptographic Module Ports and Interfaces			X		
Roles, Services and Authentication			X		
Finite State Model			X		
Physical Security			X		
Operational Environment	X				
Cryptographic Key Management			X		
EMI/EMC			X		

FIPS 140-2 Sections	Security Level				
	N/A	1	2	3	4
Self-Tests			X		
Design Assurance			X		
Mitigation of Other Attacks	X				

The Qualcomm Crypto Engine Core is classified as a single-chip hardware module for the purpose of FIPS 140-2 validation. The logical cryptographic boundary is the sub-chip implementing the Qualcomm Crypto Engine Core, while the physical boundary is the Snapdragon 888 5G Mobile Platform SoC, Qualcomm QCM6490 SoC, Qualcomm QCS6490 SoC, and Snapdragon 695 5G Mobile Platform SoC. The Qualcomm Crypto Engine Core was tested as a sub-chip implemented within the Snapdragon 888 5G Mobile Platform SoC, Qualcomm QCM6490 SoC, Qualcomm QCS6490 SoC, and Snapdragon 695 5G Mobile Platform SoC.

2.2.Description of Modes of Operations

The Qualcomm Crypto Engine Core supports two modes of operation: FIPS approved mode and a non-approved mode. The mode of operation is implicitly assumed depending on the service invoked. The Qualcomm Crypto Engine Core enters FIPS approved mode after successful completion of the power up self-tests. Invoking a non-approved service will result in the Qualcomm Crypto Engine Core implicitly switching to non-approved mode. After completion of the service the Qualcomm Crypto Engine Core will immediately switch back to the FIPS approved mode. Then depending on the next service call it will either remain in FIPS mode or will transition to non-approved mode. All Critical Security Parameters (CSP) are kept separate between the two modes.

Table 2-1 provides a summary of all security functions (both FIPS Approved and FIPS non-Approved). Table 4-1 lists the roles. Table 4-2 and Table 4-3 illustrate the services available to each role (Crypto Officer and User).

2.3.Cryptographic Module Boundary

The physical boundary of the Qualcomm Crypto Engine Core is the Snapdragon 888 5G Mobile Platform SoC, Qualcomm QCM6490 SoC, Qualcomm QCS6490 SoC, and Snapdragon 695 5G Mobile Platform SoC, which contain the Qualcomm Crypto Engine Core, which is implemented as a sub-chip. Consequently, the embodiment of the Qualcomm Crypto Engine Core is a Single-chip cryptographic module. The logical boundary is the Crypto Engine Core.

2.3.1.Hardware Block Diagram

In the hardware block diagram, the arrows depict the flow of the status, control, and data. Parameters are passed to the Qualcomm Crypto Engine Core and results received from the Qualcomm Crypto Engine Core, are via Direct Memory Access (DMA) writing and reading the registers of Qualcomm Crypto Engine Core.

The CSP, such as the encryption key, are written directly to registers or submitted via the FIFO channel to be stored within the Qualcomm Crypto Engine Core 5.6.0 hardware. Snapdragon 888 5G Mobile Platform SoC, Qualcomm QCM6490 SoC Qualcomm QCS6490 SoC, and Snapdragon 695 5G Mobile Platform SoC components outside Qualcomm Crypto Engine Core logical boundary either pass the CSP from the software executing on top of the SoC to the Qualcomm Crypto Engine

Core, or, as a “user” of cryptographic services, generates the CSP and delivers them to the Qualcomm Crypto Engine Core.

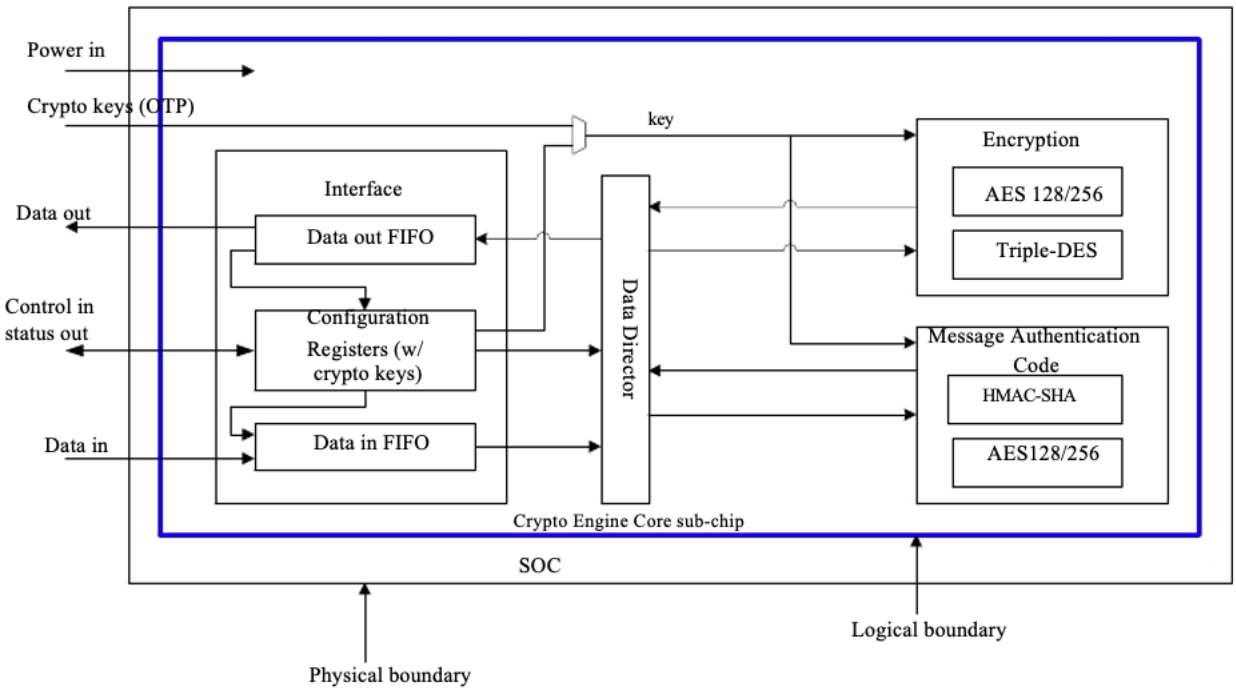


Figure 1: Hardware Block Diagram

The CSPs are passed via Direct Memory Access (DMA) to First-In First-Out queues (FIFOs) and processed by the Qualcomm Crypto Engine Core. All parameters to the Qualcomm Crypto Engine Core are also provided via FIFOs.

Figure 2: Snapdragon 888 5G Mobile Platform processor

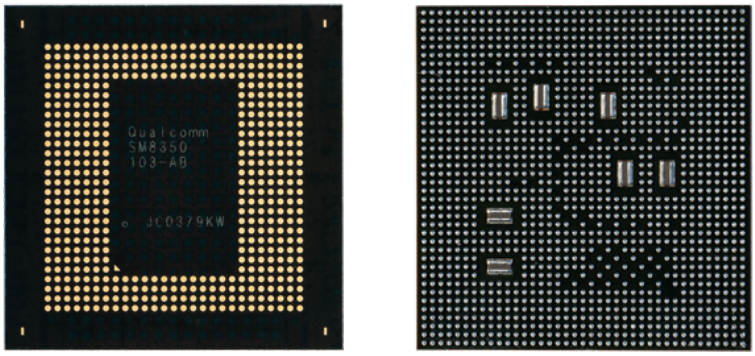


Figure 3: Qualcomm QCM6490 processor

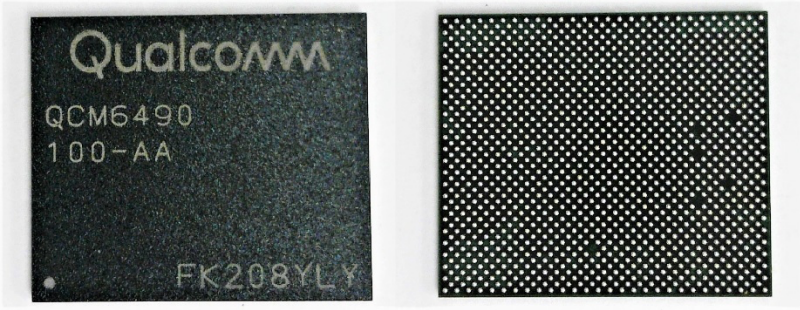


Figure 4: Qualcomm QCS6490 processor

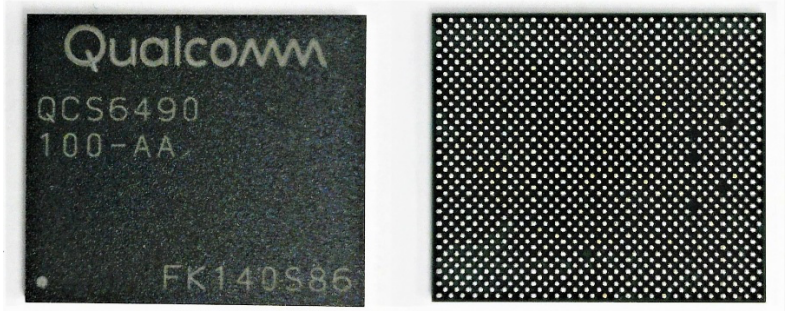
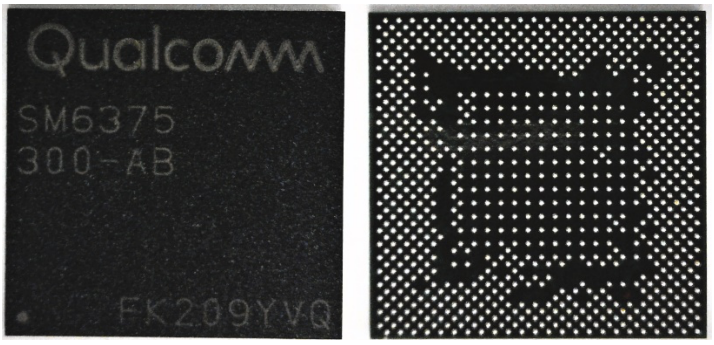


Figure 5: Snapdragon 695 5G Mobile Platform processor



3.Cryptographic Module Ports and Interfaces

Table 3-1 Ports and Interfaces

FIPS Interface	Ports
Data Input	Data in FIFOs
Data Output	Data out FIFOs
Control Input	Registers
Status Output	Registers
Power Input	Physical power connector

As indicated in Table 3-1, control input information is directed through the registers of Qualcomm Crypto Engine Core, the control input interface. For data input and data output, the FIFOs implement the high-speed interface. The status output is provided via registers.

Once the Qualcomm Crypto Engine Core finishes initialization and all self-tests complete successfully, all cryptographic functions are made available. If any of the KATs of Qualcomm Crypto Engine Core fails, the Qualcomm Crypto Engine Core self-test causes the Qualcomm Crypto Engine Core to enter into a locked state (see Section 9.1 for more details). To recover from a KAT failure a reset of the Qualcomm Crypto Engine Core is required. The reset causes it to reinitialize and re-run all KATs.

Caller-induced or internal errors do not reveal any sensitive material to callers. Cryptographic bypass capability is not supported by the Qualcomm Crypto Engine Core. 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 any entity interacting with the Qualcomm Crypto Engine Core from being able to read the CSPs. Additionally, key zeroization can be performed by issuing a reset event to the Qualcomm Crypto Engine Core. There is no means to obtain sensitive information from the Qualcomm Crypto Engine Core.

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

4.Roles, Services and Authentication

4.1.Roles

The Qualcomm Crypto Engine Core implements role-based authentication with two roles: a Crypto Officer role and a User role.

Users of the Qualcomm Crypto Engine Core are the boot loader and software applications loaded onto the Snapdragon 888 5G Mobile Platform SoC, Qualcomm QCM6490 SoC, Qualcomm QCS6490 SoC, and Snapdragon 695 5G Mobile Platform SoC. In a typical use case scenario of the Qualcomm Crypto Engine Core, an Original Equipment Manufacturer (OEM) places a hash of their RSA public key into the One-Time Programmable (OTP) memory, within the Qualcomm Crypto Engine Core upon the purchase of Snapdragon 888 5G Mobile Platform SoC, Qualcomm QCM6490 SoC, Qualcomm QCS6490 SoC, and Snapdragon 695 5G Mobile Platform SoC. The OEM uses the uniquely matching private key to sign the boot loader and software application images along with the software IDs. The OEM also includes a copy of the OEM's x.509 certificate in each signed image.

The user authentication is based on RSA signature verification and is explained in more detail in the following sections.

4.1.1.Crypto Officer Role

The boot loader acts as the Crypto Officer role when it configures the Qualcomm Crypto Engine Core by properly setting up keys/CSPs in the designated key registers or the FIFOs that will be later used by the software applications.

4.1.2.User Role

The software applications act as the User role when requesting any services provided by the Qualcomm Crypto Engine Core. The User role has access to all services of the Qualcomm Crypto Engine Core except Qualcomm Crypto Engine Core initialization.

Table 4-1 Roles

Roles	Services (see Table 4-2 and 4-3)
User	Utilization of cryptographic services of the Qualcomm Crypto Engine Core
Crypto Officer	Configure Qualcomm Crypto Engine Core keys for use by user role

4.2.Services

The Qualcomm Crypto Engine Core does not provide a bypass capability through which some cryptographic operations are not performed or where certain controls implemented during normal operation are not enforced.

All services are implemented within the Qualcomm Crypto Engine Core.

The following tables (Table 4-2 and Table 4-3) illustrate the roles and corresponding services of the Crypto Officer and User. When the services in Table 4-2 are performed, The Crypto Engine Core is in FIPS of operation. When the services in Table 4-3 are performed, the Crypto Core Engine is in non-FIPS mode of operation.

Table 4-2 Approved Services in FIPS mode

Services	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access	Standard
	User	CO					
Symmetric Algorithms							
AES encryption and decryption	✓		AES Symmetric key (128, 256 bit)	CBC, ECB, CTR, CCM, XTS	Certs. #A805, #A2752	Read	FIPS 197 SP 800-38 [A, C, E]
Triple-DES	✓		Triple DES Symmetric key (192 bits) Note: The effective bit-strength is 112 bits	CBC, ECB	Certs. #A805, #A2752	Read	FIPS 46-3 SP 800-38A
Hash Functions							
SHA-1	✓		None	N/A	Certs. #A805, #A2752	N/A	FIPS 180-4
SHA-256	✓		None	N/A	Certs. #A805, #A2752	N/A	FIPS 180-4
SHA-384	✓		None	N/A	Certs. #A805, #A2752	N/A	FIPS 180-4
SHA-512	✓		None	N/A	Certs. #A805, #A2752	N/A	FIPS 180-4
Message Authentication Codes (MACs)							
HMAC SHA-1	✓		HMAC SHA-1 key (key length between 112 bits and 512 bits)	N/A	Certs. #A805, #A2752	Read	FIPS 198-1
HMAC SHA-256	✓		HMAC SHA-256 key (key length between 112 bits and 512 bits)	N/A	Certs. #A805, #A2752	Read	FIPS 198-1

Services	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access	Standard
	User	CO					
HMAC SHA-384	✓		HMAC SHA-384 key (key length between 112 bits and 512 bits)	N/A	Certs. #A805, #A2752	Read	FIPS 198-1
HMAC SHA-512	✓		HMAC SHA-512 key (key length between 112 bits and 512 bits)	N/A	Certs. #A805, #A2752	Read	FIPS 198-1
AES-CMAC	✓		CMAC key (128, 256 bit)	CMAC	Certs. #A805, #A2752	Read	SP 800-38B
Miscellaneous							
Configure Qualcomm Crypto Engine Core keys for use by User role[1]		✓	None	N/A	N/A	N/A	N/A
Self Tests	✓		None	N/A	N/A	N/A	N/A
Zeroization	✓		All CSPs	N/A	N/A	Write	N/A
Query status	✓		None	N/A	N/A	N/A	N/A

Table 4-3 Non-Approved Services in non-FIPS mode

Services	Roles	
	User	CO
AES-GCM	✓	
DES ECB, CBC	✓	
Triple-DES (2 Key)	✓	
HMAC SHA-1 with key size less than 112 bits	✓	

[1] The methodology for setting the encryption keys is described in the “Crypto Core Hardware Programming Guide” manual

Services	Roles	
	User	CO
HMAC SHA-256 with key size less than 112 bits	✓	
HMAC SHA-384 with key size less than 112 bits	✓	
HMAC SHA-512 with key size less than 112 bits	✓	
AEAD-SHA-1 AES CBC	✓	
AEAD-SHA-1 AES CTR	✓	
AEAD-SHA-1 DES CBC	✓	
AEAD-SHA-1 Triple-DES CBC	✓	

4.3.Authentication

As mentioned previously, user authentication is based on RSA signatures. Each OEM utilizes their unique RSA private key to sign the boot loader and software application images along with its x.509 certificate. The x.509 certificate contains the OEM's public key. The OU field (i.e., the field indicating the Certification Services Division) of the signed x.509 certificate contains the software ID. Finally, the OEM puts a hash of its public key into non-volatile read-only OTP memory within the Qualcomm Crypto Engine Core.

The user is authenticated via the software ID embedded in the loadable image. The user authentication performed is twofold. First, the OEM's public key in the x.509 certificate within the image is hashed and the hash value is compared to the hash of the RSA public key stored in read-only memory within the Qualcomm Crypto Engine Core. If the hashes match, the OEM's public key is verified. Then, the OEM's public key is used to verify the RSA signature of the boot loader or the software image to be loaded. If the RSA signature verification succeeds, then the image is authenticated and hence can be loaded and executed on the Snapdragon 888 5G Mobile Platform SoC, Qualcomm QCM6490 SoC, Qualcomm QCS6490 SoC, and Qualcomm Snapdragon 695 5G Mobile Platform SoC.

4.4.Strength of Authentication

Storing a hash of the OEM's public key within the read-only memory of Qualcomm Crypto Engine Core allows the OEM to choose the size of the RSA key they want to use for authentication to the Qualcomm Crypto Engine Core. The minimum RSA key size that an OEM may use is 2048-bits. According to table 1 in FIPS IG 7.5, an RSA key size of 2048 bits provides a minimum of 112 bits of strength and a key size of 3072 bits provides a minimum of 128 bits of strength. Therefore, the probability of guessing the signing private key for this authentication mechanism is at most 1 / 2^{112} or 1.925929944e-34. The ability to successfully authenticate the RSA signed image is dependent on the ability to guess the signing RSA private key that matches the verified public key. Even using a rate of 1µs per failed authentication, which would allow 60,000,000 consecutive attempts per minute (60s / 0.00001s), only provides a probability of successfully authenticating

that is less than or equal to 60,000,000 * 1 / 2^{112} (≤6.933347799e-19) which is much less than 1 / 100,000 or 0.00001.

4.5.Authentication Data Protection

The hash of the RSA public key stored in the read-only memory of the Qualcomm Crypto Engine Core is used as the means to verify the OEM’s public key. Since this memory is non-volatile read-only memory, it cannot be modified. The verified public key is used to verify the OEM’s RSA signature of the signed boot loader or software application images. Only the images that are signed by the OEM can be authenticated to the Qualcomm Crypto Engine Core. Any image with an altered RSA signature won’t be authenticated. Hence, it won’t be loaded and get to use the Qualcomm Crypto Engine Core.

5.Physical Security

5.1.Type

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 enclosed in a production grade component.

At the time of manufacturing, the die 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 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 completely surrounds the Qualcomm Crypto Engine Core.

6.Operational Environment

6.1.Applicability

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

7.Cryptographic Key Management

7.1.Key/CSP Generation Management

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

The Qualcomm Crypto Engine Core does not provide any asymmetric algorithms. Manual key entry or key output capabilities are not provided. All Keys/CSPs 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.

Callers pass keys and similar sensitive information to the Qualcomm Crypto Engine Core by writing to specific assigned registers by sending the data via DMA request. Any attempt to write to a non-assigned FIFO is blocked. Keys are stored within the Qualcomm Crypto Engine Core in write-only registers or the internal key store of Qualcomm Crypto Engine Core. Therefore, any attempt to read CSPs are blocked, and zeros are returned rather than the actual CSP.

Keys and CSPs can be explicitly zeroized by sending an access control reset event to the Qualcomm Crypto Engine Core.

7.2.Zeroization

As stated previously, the Qualcomm Crypto Engine Core stores all keys and CSPs internally. All keys and CSPs are stored write-only and are not readable outside of the Qualcomm Crypto Engine Core. When the Qualcomm Crypto Engine Core receives a reset event, it will zeroize all CSPs contained within the Qualcomm Crypto Engine Core.

7.3.Key/CSP Lifecycle

The following table shows the generation, storage and zeroization of all CSPs used by the Qualcomm Crypto Engine Core.

Table 7-1 Key/CSP Lifecycle

Key/CSP	Generation	Storage	Zeroization
AES Keys	N/A	Internal key storage memory or Register set (legacy use)	During module reset or when overwritten by new key
Triple-DES Keys	N/A	Internal key storage memory or Register set (legacy use)	During module reset or when overwritten by new key
HMAC Keys	N/A	Internal key storage memory or Register set (legacy use)	During module reset or when overwritten by new key
CMAC Keys	N/A	Internal key storage memory or Register set (legacy use)	During module reset or when overwritten by new key

8.Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The Qualcomm Crypto Engine Core hardware component cannot be certified by the FCC, as it is not a standalone device. It is a sub-chip embedded in the Snapdragon 888 5G Mobile Platform SoC, Qualcomm QCM6490 SoC, Qualcomm QCS6490 SoC, and Snapdragon 695 5G Mobile Platform SoC, which are also not standalone devices. However, it is intended to be used within a COTS device which would undergo standard FCC certification for EMI/EMC.

According to 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, the Qualcomm Crypto Engine Core is not subject to EMI/EMC regulations because it is a subassembly that is sold to an equipment manufacturer for further fabrication. That manufacturer is responsible for obtaining the necessary authorization for the equipment with the Qualcomm Crypto Engine Core embedded prior to further marketing to a vendor or to a user.

9.Power up Tests

Power up self-tests consist of known-answer tests of algorithm implementations. The Qualcomm Crypto Engine Core power up tests are automatically performed, independently of any user during power up of the Qualcomm Crypto Engine Core. All self-tests are performed as a single atomic action that has two possible results: success or failure. If the result is success, the Qualcomm Crypto Engine Core becomes operational, if it is failure, the Qualcomm Crypto Engine Core enters into an error state and cryptographic functions cannot be performed.

The power up tests are also run when a reset event is received. If any of the tests fail, the Qualcomm Crypto Engine Core will enter into an error state. The Qualcomm Crypto Engine Core cannot be used in this state. To recover from the error state, it needs to be re-initialized. This is achieved via the successful execution of the power up tests, which can be triggered by either a power-off/power-on cycle or the receipt of a reset event.

The power up tests trigger immediately when a reset occurs and execute all needed tests until completion. Once completed successfully, the logic releases the Qualcomm Crypto Engine Core for external usage. If an error is detected during the tests, the logic locks the Qualcomm Crypto Engine Core and prevents external usage. Once locked, the Qualcomm Crypto Engine Core will only respond to a reset, which will cause the Qualcomm Crypto Engine Core to re-execute the power up tests. If the error persists, the Qualcomm Crypto Engine Core will remain unavailable.

“On demand” tests which are required by FIPS 140-2 can be performed by either of the following methods:

- A power-off/power-on cycle of the Qualcomm Crypto Engine Core
- Issuing a Crypto Core reset to the Qualcomm Crypto Engine Core

The Qualcomm Crypto Engine Core implements the following self-tests to ensure proper functioning of the Qualcomm Crypto Engine Core implemented self-tests include power up self-tests of all approved algorithms.

9.1.Cryptographic algorithm tests (known answer tests)

Table 9-2 Power up Tests

Algorithm	Test
AES encryption (CCM)	KAT
AES decryption (CCM)	KAT
AES encryption (ECB)	KAT
AES decryption (ECB)	KAT
Triple-DES encryption (ECB)	KAT
Triple-DES decryption (ECB)	KAT
HMAC SHA-1	KAT
HMAC SHA-256	KAT
AES-CMAC	KAT
HMAC SHA-384	KAT
HMAC SHA-512	KAT

10.Design Assurance

10.1.Configuration Management

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

10.1.1.Crypto Officer Guidance

The Qualcomm Crypto Engine Core does not need FIPS 140-2 specific guidance. The FIPS 140-2 functional requirements are always invoked.

For configuring the authentication mechanism as well as the access control functionality, the manual for the Qualcomm Crypto Engine Core should be used.

11. User Guidance

The operation of the Qualcomm Crypto Engine Core does not need FIPS 140-2 specific guidance. The FIPS 140-2 functional requirements are always invoked.

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

NOTE:

- In order to meet the IG A.13 requirement, the same Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit blocks of data.

- The size of the AES counter is set by a mask. The mask must either not be set (this having a 128-bit counter), or any bit mask guaranteeing that the counter is at least 64 bits in size. This will prevent a rollover.

- In order to meet IG A.9 requirement, the XTS key check to ensure key1 does not equal key2 is done prior to using the keys for the AES-XTS algorithm.

- The AES algorithm in XTS mode can be only used for the cryptographic protection of data on storage devices, as specified in [SP800-38E]. In addition, the length of a single data unit encrypted with the AES-XTS shall not exceed 2^{20} AES blocks.

12. Mitigation of Other Attacks

The Mitigation of Other Attacks security section of FIPS 140-2 is not applicable to the Qualcomm Crypto Engine Core.

13.Terms and Abbreviations

AES	Advanced Encryption Specification
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CM	Cryptographic Module
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off The Shelf
CO	Crypto Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
DMA	Direct Memory Access
FIFO	First In, First Out
FIPS	Federal Information Processing Standards Publication
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Science and Technology
OEM	Original Equipment Manufacturer
OTP	One-Time Programmable
SHA	Secure Hash Algorithm
SoC	System on Chip