Qualcomm® Inline Crypto Engine (UFS)

Versions 3.2.0, 3.2.1, 4.0.1 and 4.0.2

FIPS 140-3 Non-Proprietary Security Policy

Version 1.1

Last update: 2024-07-24

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

1 Table of Contents

1 General

1.1 This Security Policy Document

This Security Policy describes the features and design of the module named Qualcomm® Inline Crypto Engine (UFS) 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 How this Security Policy was Prepared

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

This document is the non-proprietary FIPS 140-3 Security Policy for versions 3.2.0, 3.2.1, 4.0.1 and 4.0.2 of the Qualcomm Inline Crypto Engine (UFS). It has a one-to-one mapping to the [SP 800-140B] starting with section B.2.1 named “General” that maps to section 1 in this document and ending with section B.2.12 named “Mitigation of other attacks” that maps to section 12 in this document.

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

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

Table 1 - Security Levels

2 Cryptographic Module Specification

2.1 Description of Module

The Qualcomm Inline Crypto Engine (UFS) is classified as a sub-chip hardware module in a single chip embodiment for the purpose of FIPS 140-3 validation. It provides AES-XTS encryption and decryption of block storage devices as defined in SP 800-38E. The underlying AES for AES-XTS is compliant to FIPS 197.

The Qualcomm Inline Crypto Engine (UFS) has been tested on the following platforms with the corresponding module variants and configuration options:

Model[1]	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
Snapdragon®[2] 8 Gen 1 Mobile Platform	Qualcomm Inline Crypto Engine (UFS) with version 3.2.1	N/A	N/A
Snapdragon 8+ Gen 1 Mobile Platform	Qualcomm Inline Crypto Engine (UFS) with version 3.2.1	N/A	N/A
Qualcomm® QCM6490[2]	Qualcomm Inline Crypto Engine (UFS) with version 3.2.0	N/A	N/A
Qualcomm® QCS6490[2]	Qualcomm Inline Crypto Engine (UFS) with version 3.2.0	N/A	N/A
Snapdragon 8 Gen 2 Mobile Platform	Qualcomm Inline Crypto Engine (UFS) with version 4.0.1	N/A	N/A
Snapdragon 695 5G Mobile Platform	Qualcomm Inline Crypto Engine (UFS) with version 3.2.0	N/A	N/A
Snapdragon 6 Gen 1 Mobile Platform	Qualcomm Inline Crypto Engine (UFS) with version 3.2.1	N/A	N/A
Snapdragon 8 Gen 3 Mobile Platform	Qualcomm Inline Crypto Engine (UFS) with version 4.0.2	N/A	N/A
Snapdragon 4 Gen 2 Mobile Platform	Qualcomm Inline Crypto Engine (UFS) with version 3.2.1	N/A	N/A
Snapdragon 7 Gen 1 Mobile Platform	Qualcomm Inline Crypto Engine (UFS) with version 3.2.1	N/A	N/A
Qualcomm® QCM4490[2]	Qualcomm Inline Crypto Engine (UFS) with version 3.2.1	N/A	N/A
Qualcomm® QCS4490[2]	Qualcomm Inline Crypto Engine (UFS) with version 3.2.1	N/A	N/A

[1] This column represents the SoC on which the module has been tested.

[2] Snapdragon, Qualcomm QCM6490, and Qualcomm QCS6490 are products of Qualcomm Technologies, Inc. and/or its subsidiaries.

Table 2 - Cryptographic Module Tested Configuration

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

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
A771, A2116, A2886, A4287	AES FIPS 197 AES-ECB SP 800-38A	ECB encryption	128 and 256 bits	encryption
A772, A2117, A2887, A4288		ECB decryption		decryption
A771, A2116, A2886, A4287	AES-XTS SP 800-38E	XTS encryption	128 and 256 bits	encryption
A772, A2117, A2887, A4288		XTS decryption		decryption

Table 3 - Approved Algorithms

Algorithm/Function	Use/Function
AES bitlocker	encryption/decryption

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

NOTE: the module does not implement any non-approved but allowed, or non-approved but allowed with no security claimed algorithms.

2.2 Cryptographic Module Boundary

The cryptographic boundary of the Qualcomm Inline Crypto Engine (UFS) is the sub chip component shown with blue box. The module has been tested on the platforms listed in Table 2 which form the physical perimeter for the module. Consequently, the embodiment of the Qualcomm Inline Crypto Engine (UFS) is a single-chip cryptographic module.

Below is an illustrative diagram.

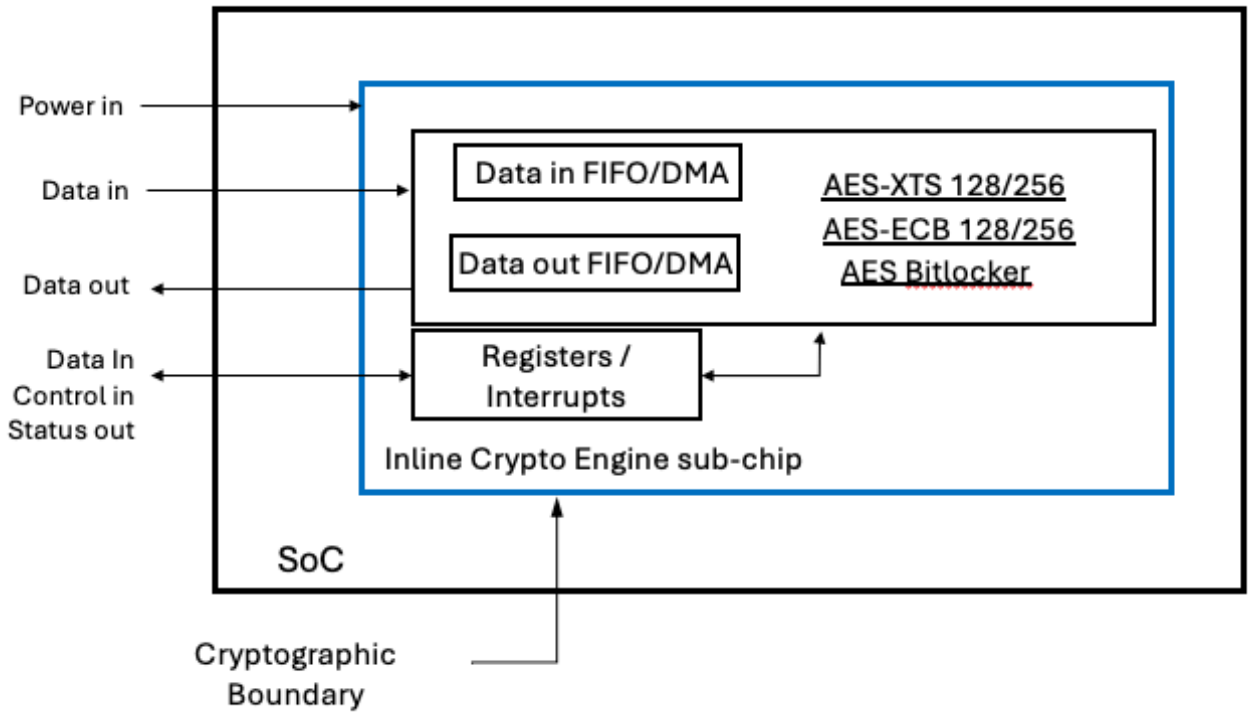

Figure 1 – Cryptographic Boundary of Qualcomm Inline Crypto Engine (UFS)

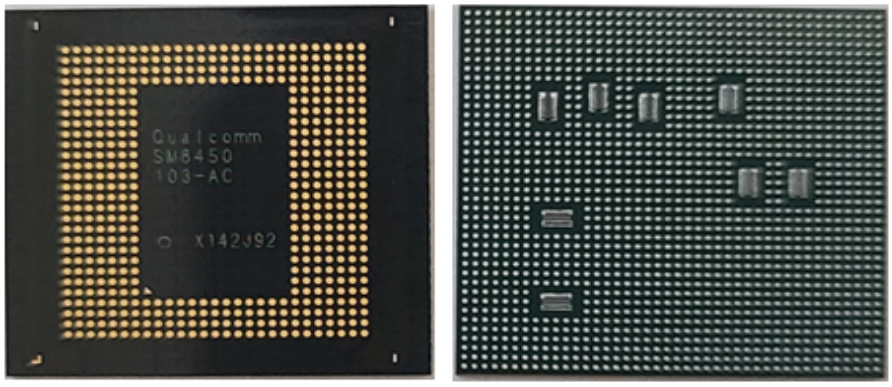

Figure 2 - Snapdragon 8 Gen 1 Mobile Platform

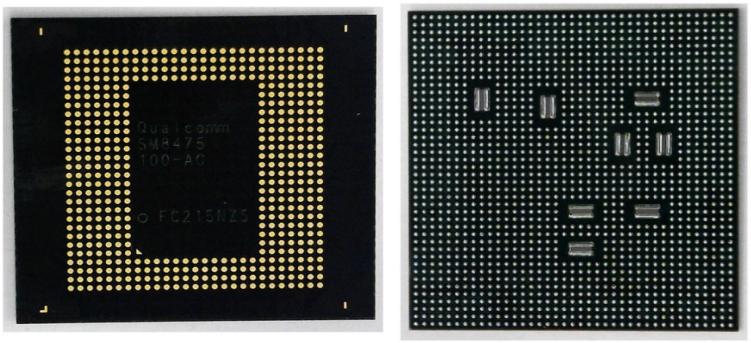

Figure 3 - Snapdragon 8+ Gen 1 Mobile Platform

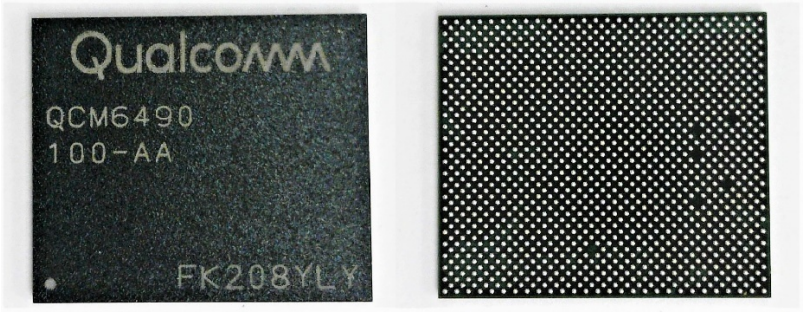

Figure 4 – Qualcomm QCM6490

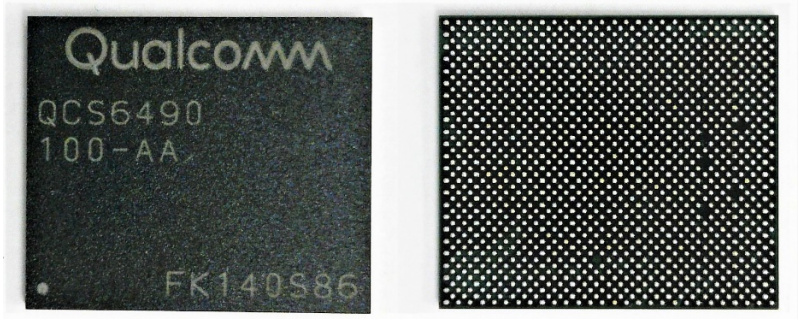

Figure 5 – Qualcomm QCS6490

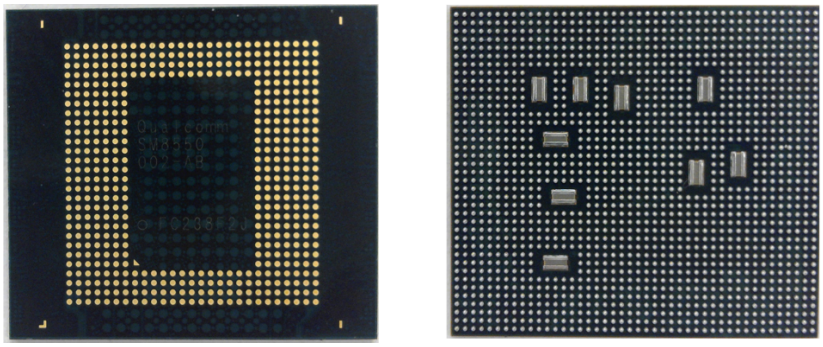

Figure 6 – Snapdragon 8 Gen 2 Mobile Platform

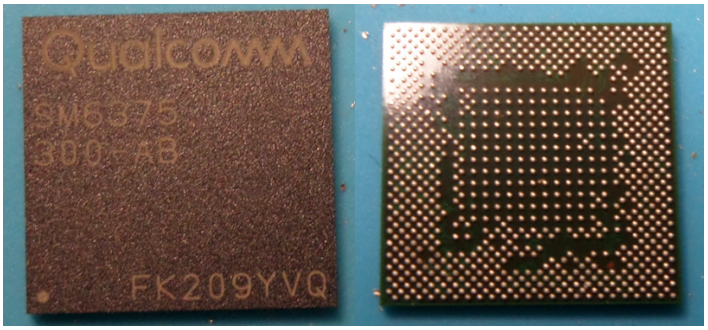

Figure 7 – Snapdragon 695 5G Mobile Platform

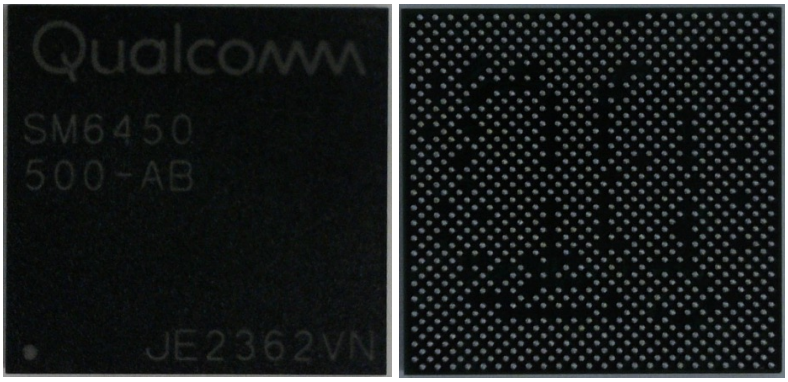

Figure 8 – Snapdragon 6 Gen 1 Mobile Platform

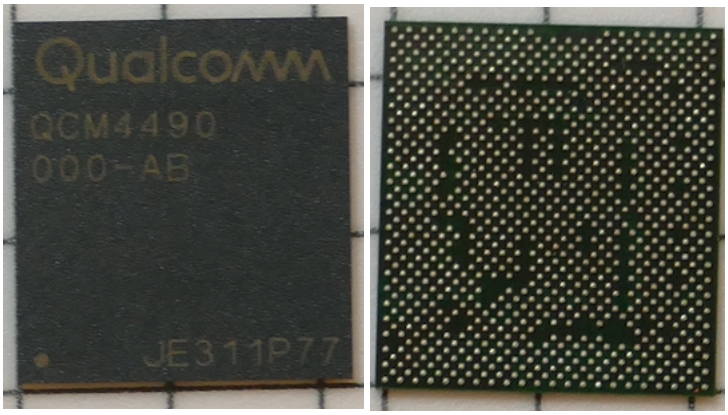

Figure 9 – Qualcomm QCM4490

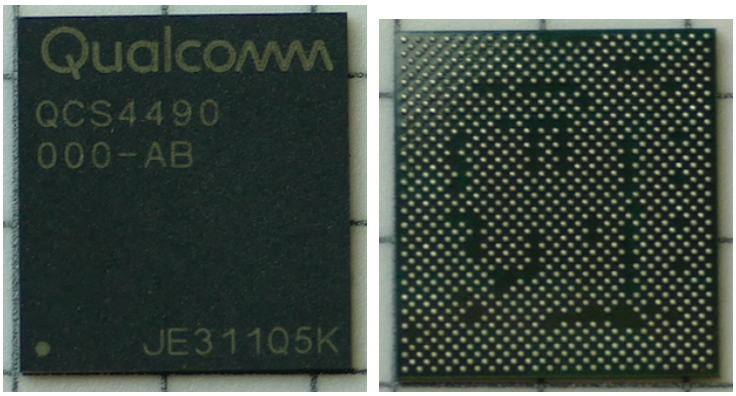

Figure 10 – Qualcomm QCS4490

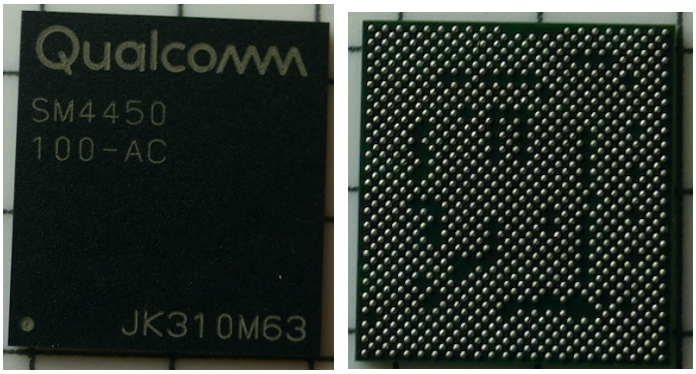

Figure 11 – Snapdragon 4 Gen 2 Mobile Platform

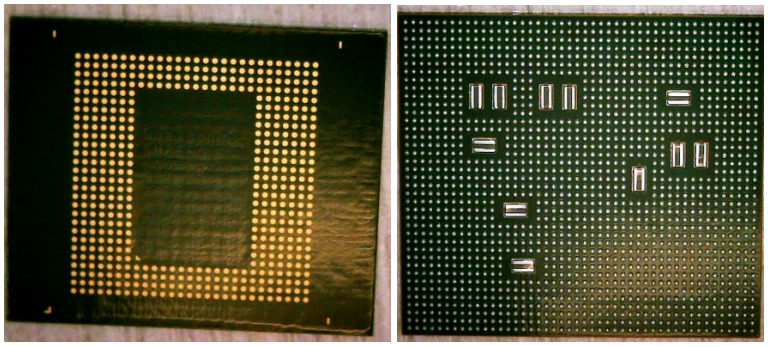

Figure 12 – Snapdragon 8 Gen 3 Mobile Platform

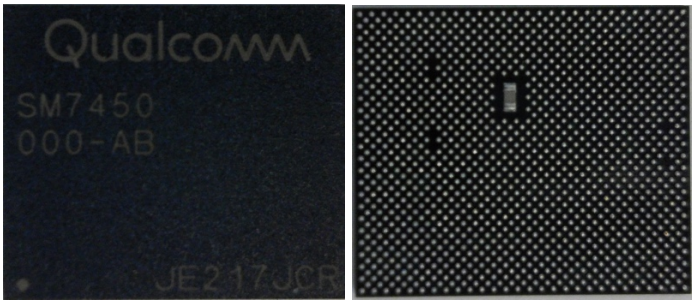

Figure 13 – Snapdragon 7 Gen 1 Mobile Platform

2.3 Mode of Operation of the Module

The Qualcomm Inline Crypto Engine (UFS) supports two modes of operation; (1) the approved mode in which the approved services are available; and (2) the non-approved mode, in which the non-approved services are available.

When the Qualcomm Inline Crypto Engine (UFS) starts up successfully, after passing all the self-tests, the module is operating in the approved mode of operation by default and can only be transitioned into the non-Approved mode by calling one of the non-Approved services listed in Table 8. Section 4 provides details on the service indicator implemented by the module. The service indicator identifies when an approved service is called.

The Qualcomm Inline Crypto Engine (UFS) can be configured to operate in one of the following two settings where the settings can be changed prior to each service request:

- Full Disk Encryption (FDE) that performs an encryption of all write operations and a decryption of all read requests with one key.

- Per-File Encryption (PFE) that performs an encryption of one write operation and a decryption of one read operation with a key dedicated to this operation.

The Qualcomm Inline Crypto Engine (UFS) supports a key storage outside of the boundary which allows up to 64 software selectable key contexts. Each context holds 2 AES keys needed for AES-XTS. One such context may be used for FDE or otherwise all 64 contexts may be used for PFE. When an encryption configuration is established, the chosen software selected context key is referenced and will be used for the operation by the Qualcomm Inline Crypto Engine (UFS).

3 Cryptographic Module Ports and Interfaces

Physical port	Logical Interface	Data that passes over port/interface
Data In FIFO/DMA	Data Input	Plaintext data that should be encrypted by the cryptographic module and ciphertext data that should be decrypted by the cryptographic module
Registers	Data Input	Cryptographic keys
Data Out FIFO/DMA	Data Output	Plaintext data that has been decrypted by the cryptographic module and ciphertext data that has been encrypted by the cryptographic module
Registers, Interrupts	Control Input	Commands input logically
Registers, Interrupts	Status Output	Status information
Physical power connector	Power Input	Power from SoC power port

Table 5 - Ports and Interfaces

As indicated in Table 5, all status output and control input are directed through the interface of the cryptographic boundary, which is the registers and interrupts of the Qualcomm Inline Crypto Engine (UFS). For data input, the Data In FIFO/DMA provides the interface. For data output, the Data Out FIFO/DMA provides the interface. The module does not implement a control output interface.

4 Roles, services, and authentication

4.1 Roles

The Crypto Officer role is assumed implicitly. Concurrent operators are not allowed.

Role	Service	Input	Output
Crypto Officer (CO)	ECB/XTS encryption	AES key, Plaintext	Ciphertext
	ECB/XTS decryption	AES key, Ciphertext	Plaintext
	Bitlocker Encryption	AES key, Plaintext	Ciphertext
	Bitlocker Decryption	AES key, Ciphertext	Plaintext
	Self-test	Module reset	Success/Fail
	Zeroization	Reset request	None
	Configuration of parameters for key	Key index	None
	Show Status	None	Return code read from register UFS_MEM_ICE_BIST_STATUS
	Show Version	None	Name and Version information read from register UFS_MEM_ICE_VERSION
	Setting encryption and decryption keys	AES key	None

Table 6 - Roles, Service Commands, Input and Output

4.2 Services

The following table describes the approved services:

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
ECB/XTS Encryption	Perform data encryption	AES-ECB 128/256 AES-XTS 128/256	AES key	CO	E, W	“UFS_MEM_ICE_PARAMETERS_4” register bits 0 and 1 indicating value 00
ECB/XTS Decryption	Perform data decryption	AES-ECB 128/256 AES-XTS 128/256				
Self-Test	Self-Test is executed automatically when device is booted or restarted	None	N/A		N/A	None
Show Version	Show the version and name of the module	None	N/A		N/A	None

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Zeroization	Zeroizes the SSP	None	AES key		Z	None
Configuration of parameters for key	Configures the registers to hold parameters such as index of the key	None	N/A		N/A	None
Status output	Show status of the module state	None	N/A		N/A	None
Setting encryption and decryption keys	Configuring the keys to be used by module	None	AES key		W	None

Table 7 - 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.

Service	Description	Algorithms Accessed	Role	Indicator
Bitlocker Encryption/Decryption	Perform data encryption/decryption	AES bitlocker	CO	“UFS_MEM_ICE_PARAMETERS_5” register bit 0 indicating value 0

Table 8 - Non-Approved Services

4.3 Operator Authentication

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

5 Software/Firmware security

The Qualcomm Inline Crypto Engine (UFS) does not support any software or firmware component. Therefore, this section is not applicable.

6 Operational Environment

6.1 Applicability

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

7 Physical Security

The Qualcomm Inline Crypto Engine (UFS) 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 circuity of the Qualcomm Inline Crypto Engine (UFS). 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 Inline Crypto Engine (UFS) 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 Inline Crypto Engine (UFS).

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

8 Non-invasive Security

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

9 Sensitive Security Parameter Management

9.1 SSP List

These keys are generated outside the boundary and set up by the Crypto Officer in the registers of the Qualcomm Inline Crypto Engine (UFS).

The following table lists the key/CSP used by the :

Key/SSP Name /Type	Strength	Security Function and Cert. Number	Generation	Import /Export	Establish-ment	Storage	Zero-ization	Use and related keys
AES key	128 and 256 bits	AES ECB/XTS Certs. #A771, #A772, #A2116, #A2117, #A2886, #A2887, #A4287, #A4288	N/A	MD/EE Import: Provided by caller. Export: N/A	N/A	Hardware registers	Zeroized during module reset	Encryption and decryption

Table 9 - SSPs

9.2 SSP Generation

The Qualcomm Inline Crypto Engine (UFS) does not provide any SSP generation or SSP establishment methods.

9.3 SSP Entry and Output

The caller provides the AES keys for encryption and/or decryption. These keys are input to the module in plaintext form by the entity residing within the same physical perimeter of the SoC on which the Qualcomm Inline Crypto Engine (UFS) runs. The module does not output any SSPs.

9.4 SSP Storage

The module does not provide persistent storage of SSPs. The SSP i.e., the AES keys are provided by the caller are set up by the CO and are temporarily stored in hardware registers. Once the keys are written to the registers, they are not readable from outside the Qualcomm Inline Crypto Engine (UFS).

9.5 SSP Zeroization

When the Qualcomm Inline Crypto Engine (UFS) performs a module reset, it will zeroize all SSPs contained within itself. The registers for the SSPs will implicitly be set to zero upon the reset, indicating the zeroization was successful.

10 Self-tests

10.1 Pre-Operational Tests

The integrity test is not applicable since the Qualcomm Inline Crypto Engine (UFS) is implemented in hardware and is non-modifiable. There are no bypass or critical function tests.

10.2 Conditional Tests

Algorithm	Test
AES-256 Encryption (ECB)	KAT
AES-256 Decryption (ECB)	KAT

Table 10 – Conditional Self-Tests

Conditional tests are performed automatically without any operator intervention during power-up of the Qualcomm Inline Crypto Engine (UFS); these tests ensure that the cryptographic algorithms work as expected. While the conditional tests are executing, services are not available, and input and output are inhibited.

10.3 On-demand Self-Test

On demand self-tests can be invoked by powering-off and reloading the module or when a reset event is received. This test performs the same conditional tests that are performed during power-up. During the execution of the on-demand self-tests, cryptographic services are not available, and no data output or input is possible.

10.4 Error States

If any of the conditional self-tests or on-demand test fails, the Qualcomm Inline Crypto Engine (UFS) will enter the error state. Data output is prohibited, and no further cryptographic operation is allowed in the error state. This is performed by the control logic that and prevents external usage when an error is detected.

To recover from the error state, re-initialization is possible by 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. Once locked, the Qualcomm Inline Crypto Engine (UFS) will only respond to a reset which will cause it to re-execute the power up tests. If the error persists, the Qualcomm Inline Crypto Engine (UFS) will remain unavailable.

Error State	Cause of Error	Status Indicator
Error	Known Answer test failure	BIST_FAILURE indicator is set

Table 11 - Error States

11 Life-cycle assurance

11.1 Delivery and Operation

The Qualcomm Inline Crypto Engine (UFS) is a sub-chip module that runs on the platforms listed in Table 2. These SoCs are delivered from the vendor via a trusted delivery courier.
On the reception of the SoC, the operator shall first check all sides of the box to verify that it has not been tampered during the shipment. Then, after opening the box the operator shall verify that the moisture barrier bag is still sealed and does not present any trace of tampering. Finally, after retrieving the SoC, the operator shall perform a visual inspection of the external package of the module, it should look similar to the pictures in Figure 2 through Figure 13.
If one of these verifications fail, the operator shall contact their Qualcomm representative which released the delivery before operating the module.
Once the product is received by the customer and powered up the test defined in section 10 will be executed.

11.2 End of Life

As stated in section 9.4, the module does not perform persistent storage of SSPs. SSP values only exists in volatile memory and these values are zeroized when the module is reset. The procedure for secure sanitization of the module at the end of life is simply to power it off, which is the action of zeroization of the SSPs. As a result of this sanitization via power-off, the SSPs are removed from the module, so that the module may either be distributed to other operators or disposed.

11.3 Crypto Officer Guidance

There is no specific crypto officer guidance required for the module.

Note: AES XTS

The module does not support AES-XTS with data unit lengths greater than 2^20 AES blocks.

To meet the requirement stated in IG C.I, the module implements a check to ensure that the two AES keys used in AES XTS mode are not identical.

The XTS mode shall only be used for the cryptographic protection of data on storage devices. It shall not be used for other purposes, such as the encryption of data in transit.

11.4 Configuration Management

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

12 Mitigation of other attacks

The Qualcomm Inline Crypto Engine (UFS) does not implement security mechanisms to mitigate other attacks.

Appendix A. Glossary and Abbreviations

AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standards Publication
FSM	Finite State Model
KAT	Known Answer Test
NIST	National Institute of Science and Technology
SoC	System on a Chip
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**
September 2020
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

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

SP800-38E **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

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