Qualcomm Technologies, Inc.

Qualcomm® Inline Crypto Engine (UFS)

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.0

Last Update: 2026-04-15

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

https://www.atsec.com

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This Security Policy describes the features and design of the module named Qualcomm® 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 Security Levels

Section	Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	N/A
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	2
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

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 module includes separate AES Engines for encryption and decryption for both ECB and XTS mode.

Module Type: Hardware

Module Embodiment: Single Chip

Module Characteristics: SubChip

Cryptographic Boundary:

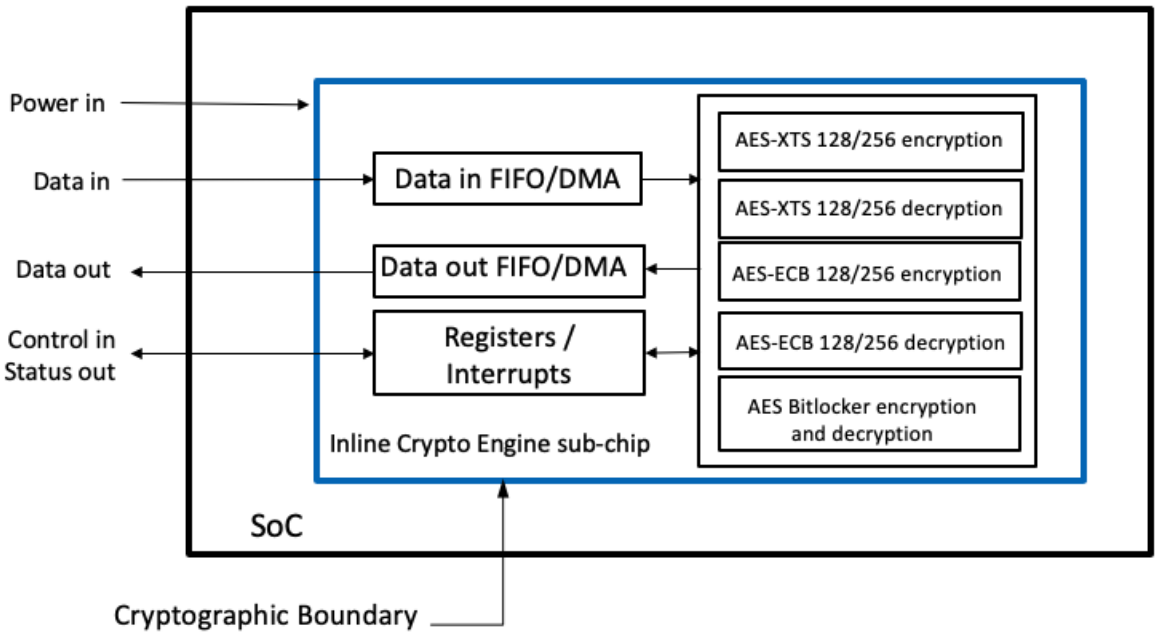

Figure 1: Cryptographic boundary and physical perimeter

Tested Operational Environment's Physical Perimeter (TOEPP):

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

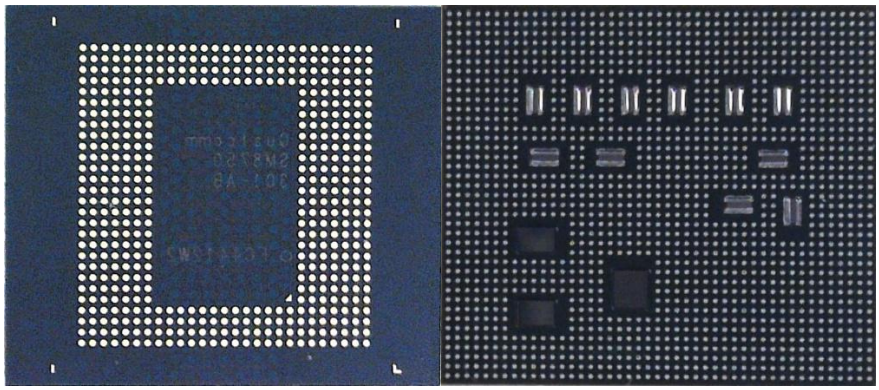

Figure 2: Snapdragon 8 Elite Mobile Platform

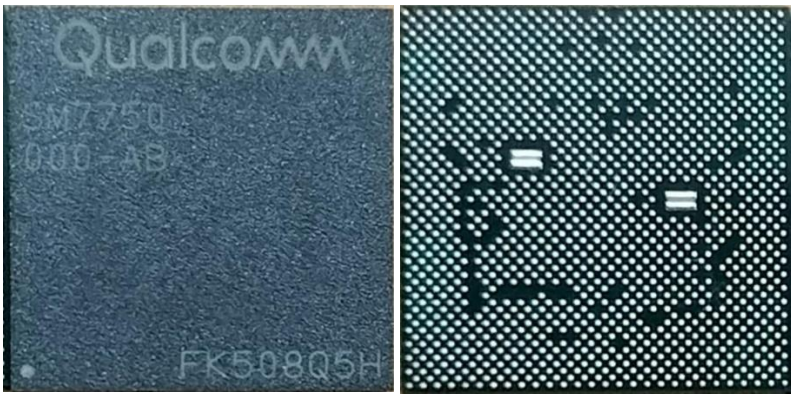

Figure 3: Snapdragon 7 Gen 4 Mobile Platform

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 Elite Mobile Platform	4.0.3	N/A	Snapdragon® 8 Elite Mobile Platform	N/A
Snapdragon® 7 Gen 4 Mobile Platform	4.0.3	N/A	Snapdragon® 7 Gen 4 Mobile Platform	N/A

Table 2: Tested Module Identification – Hardware

Snapdragon is a product of Qualcomm Technologies, Inc. and/or its subsidiaries.

2.3 Excluded Components

There are no excluded components.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode of operation	Automatically entered whenever an approved service is requested	Approved	UFS_MEM_ICE_PARAMETERS_4 register bits 0 and 1 show the value of 00
Non-approved mode of operation	Automatically entered whenever a non-approved service is requested	Non-Approved	UFS_MEM_ICE_PARAMETERS_5 register bit 30 shows the value of 1

Table 3: Modes List and Description

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.

Mode Change Instructions and Status:

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 the non-approved, not allowed algorithms table. 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 SoC supports an internal key storage which is outside the module boundary. This key storage is accessed by the caller of the module within the SoC to provide SSPs to the module. The module does not have direct access to the key storage and only communicates with the caller within the SoC.

The storage within the SoC 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).

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A6449	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A6456	Direction - Decrypt Key Length - 128, 256	SP 800-38A
AES-XTS Testing Revision 2.0	A6449	Direction - Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A6456	Direction - Decrypt Key Length - 128, 256	SP 800-38E

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
AES BitLocker	encryption, decryption

Table 5: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES-ECB	BC-UnAuth	AES in ECB mode		AES-ECB: (A6449, A6456)
AES-XTS	BC-UnAuth	AES in XTS mode		AES-XTS Testing Revision 2.0: (A6449, A6456)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES XTS

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

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

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

2.8 RBG and Entropy

The module does not employ a RBG and does not obtain entropy from any source.

2.9 Key Generation

Not Applicable. The key generation is not implemented.

2.10 Key Establishment

Not Applicable. The key establishment is not implemented.

2.11 Industry Protocols

Not applicable. There is no industry protocol implemented.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Data In FIFO/DMA, registers	Data Input	Keys, plaintext, ciphertext
Data Out FIFO/DMA	Data Output	plaintext, ciphertext
Registers, Interrupts	Control Input	Command input
Registers, Interrupts	Status Output	Status information
Physical power connector	Power	N/A

Table 7: Ports and Interfaces

The module does not implement a control output interface.

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	None

Table 8: Roles

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

The module does not support concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES Encryption	Perform data encryption	UFS_MEM_ICE_PARAMETERS_4 register bits 0 and 1 indicating value 00	AES Key, Plaintext	Ciphertext	AES-ECB AES-XTS	Crypto Officer - AES key: W,E
AES Decryption	Perform data decryption	UFS_MEM_ICE_PARAMETERS_4 register bits 0 and 1 indicating value 00	AES Key, Ciphertext	Plaintext	AES-ECB AES-XTS	Crypto Officer - AES key: W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show Status	Return code read from register UFS_MEM_ICE_BIST_STATUS (0 indicates operational, non-zero indicates error).	None	None	Module status	None	Crypto Officer
Self-Test	Self-Tests are executed automatically when device is booted or restarted	None	None	Self-test Success/Fail	None	Crypto Officer
Zeroization	Zeroizes all SSPs	None	None	None	None	Crypto Officer - AES key: Z
Configure keys for use by Crypto Officer	Configures the keys for Crypto Officer role	None	AES Key	Success/Fail	None	Crypto Officer - AES key: W
Show identifier and	Show the module identifier and module version	None	None	Identifier and Version information read from registers UFS_MEM_ICE_MODULE_IDENTIFIER and	None	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
version				UFS_MEM_ICE_VERSION		

Table 9: Approved Services

G = **Generate**: The module generates or derives the SSP.

E = Execute: The module uses the SSP in performing a cryptographic operation.

R = **Read**: The SSP is read from the module (e.g., the SSP is output).

W = **Write**: The SSP is updated, imported, or written to the module.

Z = **Zeroize**: The module zeroizes the SSP.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
BitLocker Encryption/Decryption	Perform data encryption/decryption	AES BitLocker	CO

Table 10: Non-Approved Services

4.5 External Software/Firmware Loaded

Not Applicable. No external software or firmware is loaded.

5 Software/Firmware Security

5.1 Integrity Techniques

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

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Non-Modifiable

7 Physical Security

7.1 Mechanisms and Actions Required

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

Table 11: Mechanisms and Actions Required

The Qualcomm 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 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 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

8.1 Mitigation Techniques

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 12: Storage Areas

The module does not provide persistent storage of SSPs. The SSPs 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).

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input parameter	Caller within the physical perimeter	Registers	Plaintext	Manual	Electronic	

Table 13: SSP Input-Output Methods

9.3 SSP Zeroization Methods

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

Table 14: SSP Zeroization Methods

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.

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-ECB AES-XTS

Table 15: SSP Table 1

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

Table 16: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

N/A for this module.

The integrity test is not applicable since the Qualcomm Inline Crypto Engine (UFS) is implemented in hardware and is non-modifiable.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A6449)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A6456)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	

Table 17: 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 Periodic Self-Test Information

N/A for this module.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A6449)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A6456)	KAT	CAST	On demand	Manually by power cycling

Table 18: Conditional Periodic Information

10.4 Error States

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

Table 19: Error States

If any of the 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 locks the Qualcomm Inline Crypto Engine (UFS) 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. If the error persists, the Qualcomm Inline Crypto Engine (UFS) will remain unavailable.

10.5 Operator Initiation of Self-Tests

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

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The Qualcomm Inline Crypto Engine (UFS) is a sub-chip module that runs on the SoCs listed in Table 2.

The vendor uses a trusted delivery courier to transport the SoC to their customers. On the reception of the SoC, the operator shall first check all sides of the box to verify that it has not been tampered with during the shipment. Then, after opening the box the operator shall verify that the moisture barrier bag is still sealed and does not present any trace of tampering. Finally, after retrieving the SoC, the operator shall perform a visual inspection of the external package of the module; it should look like the picture in Figures 2 or 3.

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 UFS_MEM_ICE_MODULE_IDENTIFIER and UFS_MEM_ICE_VERSION registers. The UFS_MEM_ICE_MODULE_IDENTIFIER register must hold the value 0x00000003, which identifies the module as the Qualcomm Inline Crypto Engine (UFS). The UFS_MEM_ICE_VERSION register must hold the value 0x04000003, representing the module version 4.0.3.

See section 2.7.1 for information on AES-XTS.

11.3 Non-Administrator Guidance

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

11.4 End of Life

As stated in section 9.1, the module does not perform persistent storage of SSPs. SSP values only exist 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.

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**
April 2025
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-ig-announcements

FIPS197 **Advanced Encryption Standard**
November 2001
https://doi.org/10.6028/NIST.FIPS.197-upd1

SP800-38A **NIST Special Publication 800-38A - Recommendation for Block Cipher Modes of Operation Methods and Techniques**
December 2001
https://doi.org/10.6028/NIST.SP.800-38A

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
https://doi.org/10.6028/NIST.SP.800-38E

SP800-140B **NIST Special Publication 800-140Br1 - CMVP Security Policy Requirements**
November 2023
https://doi.org/10.6028/NIST.SP.800-140Br1