Qualcomm Technologies, Inc.

Qualcomm® Inline Crypto Engine (UFS)

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 1.1

Last Update: 2026-04-06

Prepared by:

atsec information security corporation

4516 Seton Center Pkwy, Suite 250

Austin, TX 78759

https://www.atsec.com

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

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.

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:

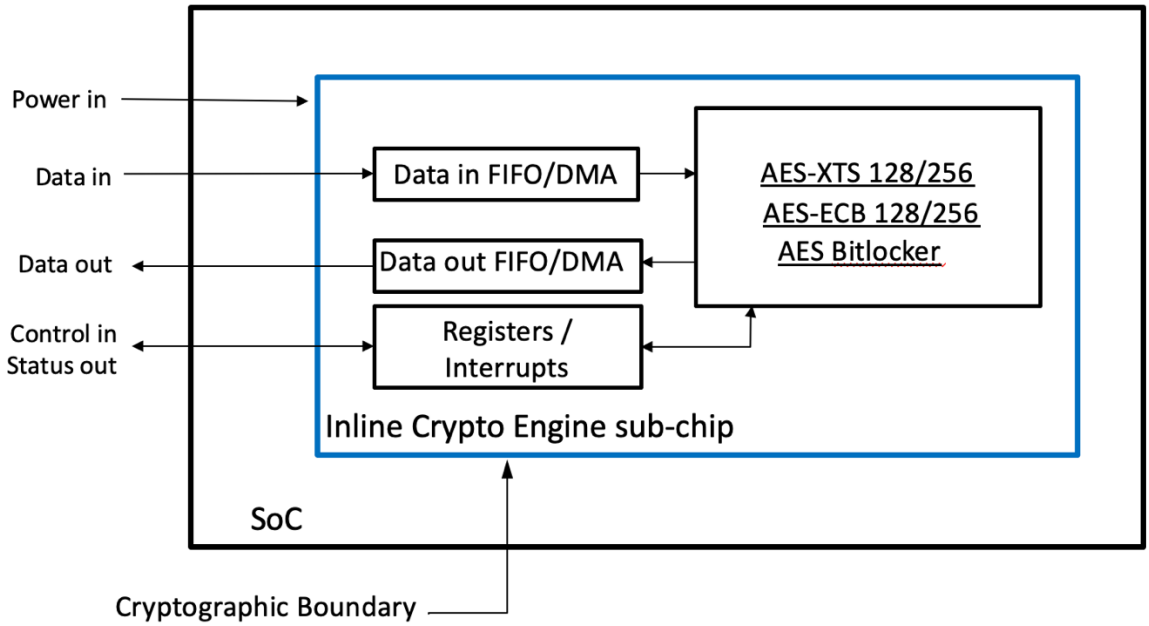

Figure 1: Cryptographic boundary and physical perimeter

Tested Operational Environment's Physical Perimeter (TOEPP):

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

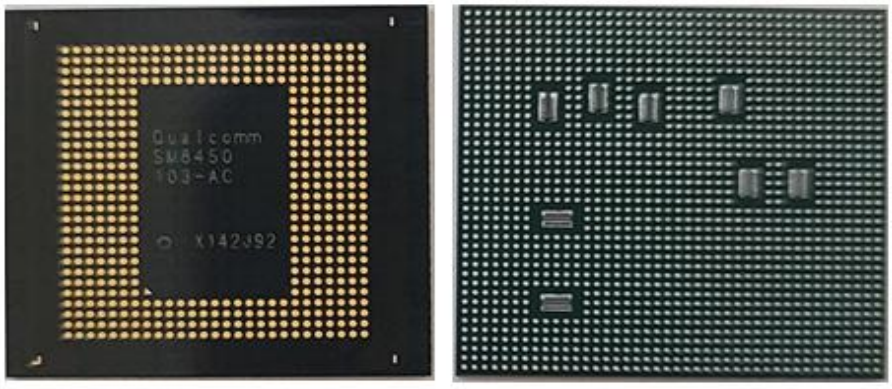

Figure 2: Snapdragon 8 Gen 1 Mobile Platform

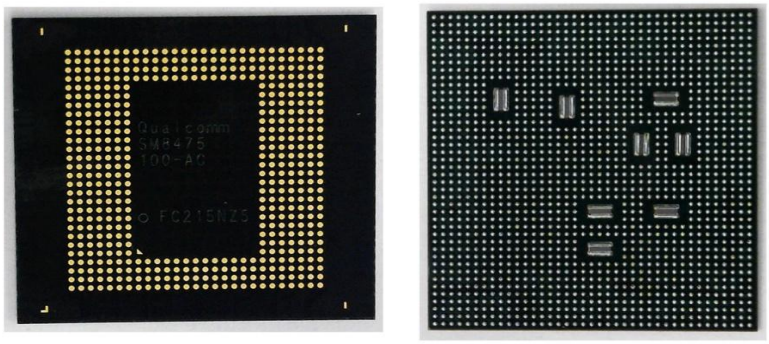

Figure 3 - Snapdragon 8+ Gen 1 Mobile Platform

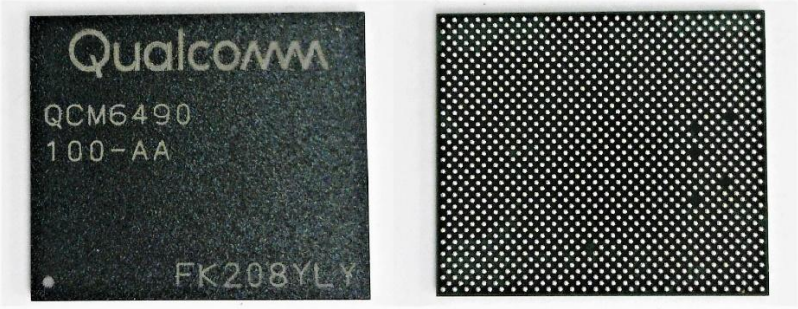

Figure 4 – Qualcomm QCM6490

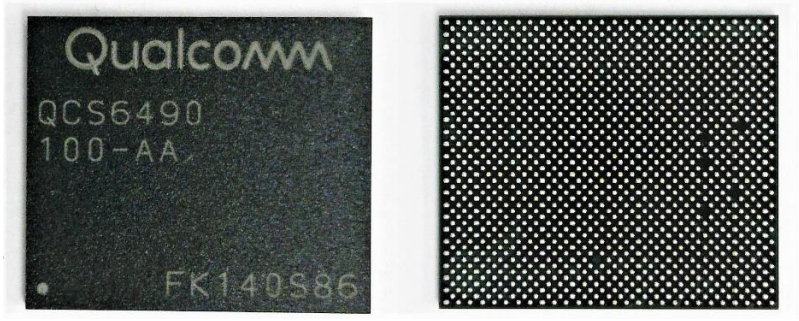

Figure 5 – Qualcomm QCS6490

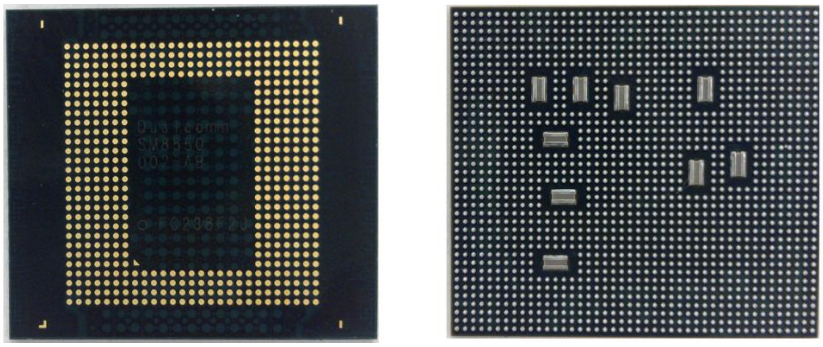

Figure 6 – Snapdragon 8 Gen 2 Mobile Platform

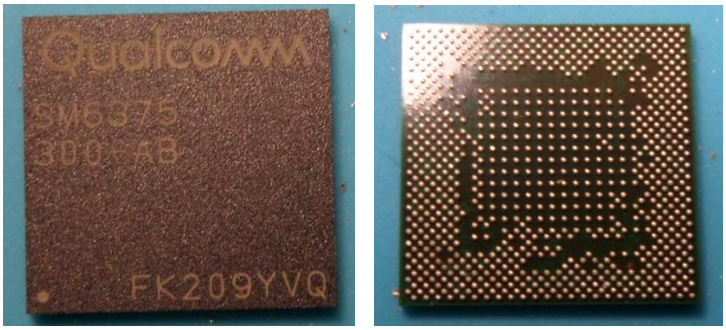

Figure 7 – Snapdragon 695 5G Mobile Platform

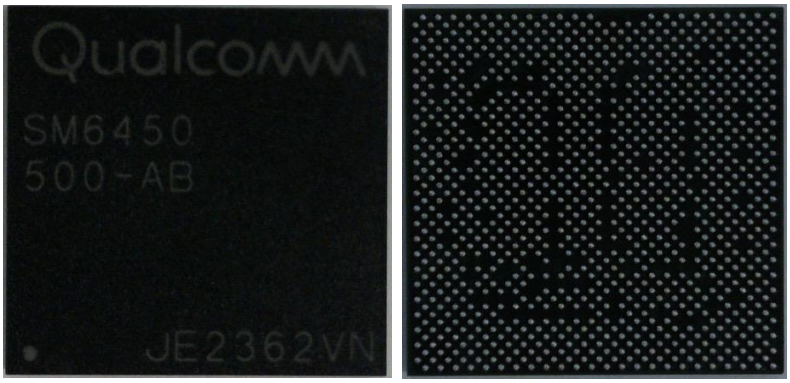

Figure 8 – Snapdragon 6 Gen 1 Mobile Platform

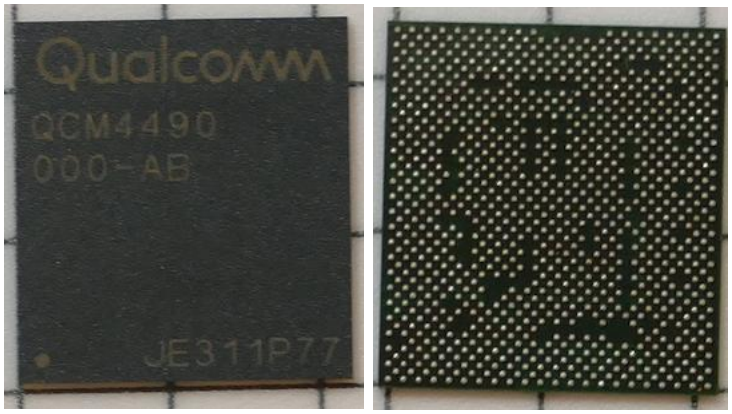

Figure 9 – Qualcomm QCM4490

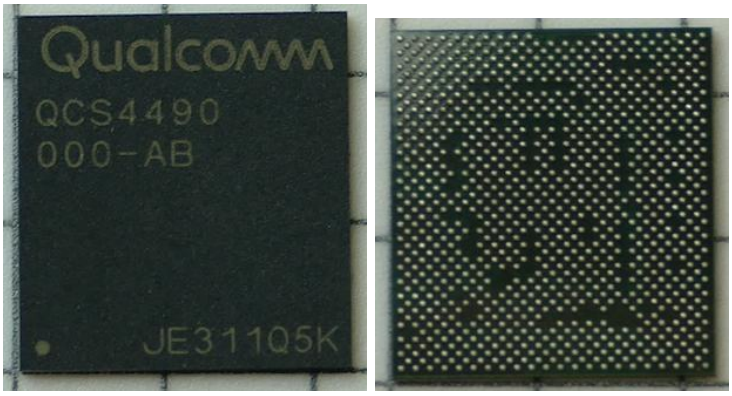

Figure 10 – Qualcomm QCS4490

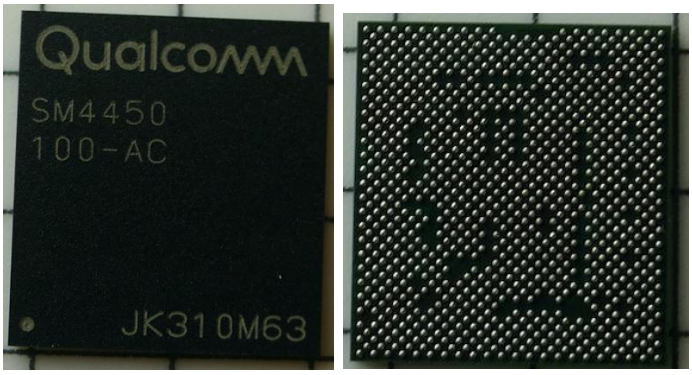

Figure 11 – Snapdragon 4 Gen 2 Mobile Platform

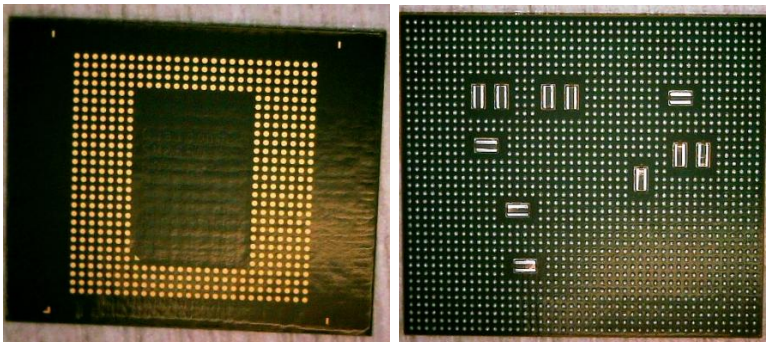

Figure 12 – Snapdragon 8 Gen 3 Mobile Platform

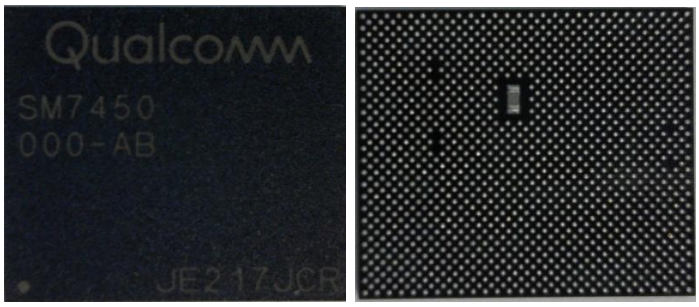

Figure 13 – Snapdragon 7 Gen 1 Mobile Platform

2.2 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 1 Mobile Platform	3.2.1	N/A	Snapdragon® 8 Gen 1 Mobile Platform	N/A
Snapdragon 8+ Gen 1 Mobile Platform	3.2.1	N/A	Snapdragon 8+ Gen 1 Mobile Platform	N/A
Qualcomm® QCM6490	3.2.0	N/A	Qualcomm® QCM6490	N/A
Qualcomm® QCS6490	3.2.0	N/A	Qualcomm® QCS6490	N/A
Snapdragon 8 Gen 2 Mobile Platform	4.0.1	N/A	Snapdragon 8 Gen 2 Mobile Platform	N/A
Snapdragon 695 5G Mobile Platform	3.2.0	N/A	Snapdragon 695 5G Mobile Platform	N/A
Snapdragon® 6 Gen 1 Mobile Platform	3.2.1	N/A	Snapdragon® 6 Gen 1 Mobile Platform	N/A
Snapdragon® 8 Gen 3 Mobile Platform	4.0.2	N/A	Snapdragon® 8 Gen 3 Mobile Platform	N/A
Snapdragon® 7 Gen 1 Mobile Platform	3.2.1	N/A	Snapdragon® 7 Gen 1 Mobile Platform	N/A
Qualcomm® QCM4490	3.2.1	N/A	Qualcomm® QCM4490	N/A
Qualcomm® QCS4490	3.2.1	N/A	Qualcomm® QC4490	N/A
Snapdragon® 4 Gen 2 Mobile Platform	3.2.1	N/A	Snapdragon® 4 Gen 2 Mobile Platform	N/A

Table 2: Tested Module Identification – Hardware

Snapdragon, Qualcomm QCM6490, Qualcomm QCS6490, Qualcomm QCS4490, and Qualcomm QCM4490 are products of Qualcomm Technologies, Inc. and/or its subsidiaries.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

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	0
Non-approved mode of operation	Automatically entered whenever a non-approved service is requested	Non-Approved	1

Table 3: Modes List and Description

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 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).

Degraded Mode Description:

N/A for this module.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	A2116	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A2117	Direction - Decrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A2886	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A2887	Direction - Decrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A4287	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A4288	Direction - Decrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A771	Direction - Encrypt Key Length - 128, 256	SP 800-38A
AES-ECB	A772	Direction - Decrypt Key Length - 128, 256	SP 800-38A
AES-XTS	A771	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536 Tweak Mode - Number	SP 800-38E
AES-XTS	A772	Direction - Decrypt Key Length - 128, 256 Payload Length - Payload Length: 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536 Tweak Mode - Number	SP 800-38E
AES-XTS Testing Revision 2.0	A2116	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A2117	Direction - Decrypt Key Length - 128, 256 Payload Length - Payload Length: 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A2886	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A2887	Direction - Decrypt Key Length - 128, 256 Payload Length - Payload Length: 512, 1024, 2048,	SP 800-38E

Algorithm	CAVP Cert	Properties	Reference
		4096, 8192, 16384, 32768, 65536 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	
AES-XTS Testing Revision 2.0	A4287	Direction - Encrypt Key Length - 128, 256 Payload Length - Payload Length: 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	SP 800-38E
AES-XTS Testing Revision 2.0	A4288	Direction - Decrypt Key Length - 128, 256 Payload Length - Payload Length: 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536 Tweak Mode - Number Data Unit Length Matches Payload Length - Yes	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	Reference:FIPS 197, SP800-38A	AES-ECB: (A2116, A2117, A2886,

Name	Type	Description	Properties	Algorithms
				A2887, A4287, A4288, A771, A772)
AES-XTS	BC-UnAuth	AES in XTS mode	Reference:FIPS 197, SP800-38E	AES-XTS Testing Revision 2.0: (A2116, A2117, A2886, A2887, A4287, A4288) AES-XTS: (A771, A772)

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.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

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	All input data
Data Out FIFO/DMA	Data Output	All data output except Status information
Registers, interrupts	Control Input	Command input
Registers, interrupts	Status Output	Status information
Physical power connector	Power	Power from SoC power port

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.

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, Success/Fail	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, Success/Fail	AES-ECB AES-XTS	Crypto Officer - AES key: W,E
Show Status	Return code read from register UFS_MEM_ICE_BIST_STATUS	None	N/A	Module status	None	Crypto Officer
Self-Test	Self-Tests are executed automatically when	None	None	Self-test Success/Fail	None	Crypto

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	device is booted or restarted					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 version	Show the version and name of the module	None	None	Name and Version information read from register UFS_MEM_ICE_VERSION	None	Crypto Officer
Setting encryption and decryption keys	Configuring the keys to be used by module	None	AES Key	None	None	Crypto Officer - AES key: W

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 support 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 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

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 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).

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input parameter	Caller within the physical perimeter	Hardware register	Plaintext	N/A	N/A	

Table 13: SSP Input-Output Methods

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.

9.3 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

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	Symmetric key used for encryption, decryption	128 or 256 bits - 128 or 256 bits	Symmetric key - CSP			AES-ECB

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						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. There are no bypass or critical function tests.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A2116)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A2117)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-ECB (A2886)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A2887)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-ECB (A4287)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A4288)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up
AES-ECB (A771)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Encryption	Performed during module power-up
AES-ECB (A772)	256 bit key	KAT	CAST	Module becomes operational and services are available for use	Decryption	Performed during module power-up

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 (A2116)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A2117)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A2886)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A2887)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A4287)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A4288)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A771)	KAT	CAST	On demand	Manually by power cycling
AES-ECB (A772)	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 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.

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 platforms covered in Table 2. The vendor uses a trusted delivery courier to transport the SoC to their customers. On the reception of the SoC, the operator shall first check all sides of the box to verify that it has not been tampered with during the shipment. Then, after opening the box the operator shall verify that the moisture barrier bag is still sealed and does not present any trace of tampering. Finally, after retrieving the SoC, the operator shall perform a visual inspection of the external package of the module; it should look like the picture in Figure 2 through Figure 13. 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

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

Note: See section 2.7.1 for AES-XTS information.

11.3 Non-Administrator Guidance

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

11.4 Design and Rules

N/A Therefore no specific design or rules to be followed.

11.5 Maintenance Requirements

N/A There are no maintenance requirements.

11.6 End of Life

As stated in section 9.1, 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.

11.7 Additional Information

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

12.1 Attack List

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