Qualcomm Technologies, Inc.

Qualcomm® Inline Crypto Engine (UFS)

FIPS 140-3 Non-Proprietary Security Policy

Prepared by:
atsec information security corporation
4516 Seton Center Parkway, Suite 250
Austin, TX 78759
www.atsec.com

Table of Contents

1 General 5

1.1 Overview 5

1.2 Security Levels 5

1.3 Additional Information 5

2 Cryptographic Module Specification 6

2.1 Description 6

2.2 Tested and Vendor Affirmed Module Version and Identification 7

2.3 Excluded Components 8

2.4 Modes of Operation 8

2.5 Algorithms 9

2.6 Security Function Implementations 9

2.7 Algorithm Specific Information 10

2.8 RBG and Entropy 10

2.9 Key Generation 10

Not Applicable. The key generation is not implemented. 10

2.10 Key Establishment 10

Not Applicable. The key establishment is not implemented. 10

2.11 Industry Protocols 10

Not Applicable. There is no industry protocol implemented. 10

3 Cryptographic Module Interfaces 11

3.1 Ports and Interfaces 11

4 Roles, Services, and Authentication 12

4.1 Authentication Methods 12

4.2 Roles 12

4.3 Approved Services 12

4.4 Non-Approved Services 13

4.5 External Software/Firmware Loaded 13

5 Software/Firmware Security 14

5.1 Integrity Techniques 14

6 Operational Environment 15

6.1 Operational Environment Type and Requirements 15

7 Physical Security 16

7.1 Mechanisms and Actions Required 16

8 Non-Invasive Security 17

8.1 Mitigation Techniques 17

9 Sensitive Security Parameters Management 18

9.1 Storage Areas 18
9.2 SSP Input-Output Methods 18
9.3 SSP Zeroization Methods 18
9.4 SSPs 18
10 Self-Tests 20
10.1 Pre-Operational Self-Tests 20
10.2 Conditional Self-Tests 20
10.3 Periodic Self-Test Information 20
10.4 Error States 21
11 Life-Cycle Assurance 22
11.1 Installation, Initialization, and Startup Procedures 22
11.2 Administrator Guidance 22
11.3 Non-Administrator Guidance 22
11.4 Design and Rules 22
11.5 Maintenance Requirements 22
11.6 End of Life 22
11.7 Additional Information 22
12 Mitigation of Other Attacks 23
12.1 Attack List 23

List of Tables

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

List of Figures

Figure 1: Block Diagram ... 6
Figure 2: Snapdragon® XR2 Gen 2 Platform ... 7
Figure 3: Snapdragon X Elite Compute Platform ... 7
Figure 4: Snapdragon X1 Plus ... 7

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for versions 3.2.1 and 4.0.1 of the Qualcomm® [1] Inline Crypto Engine (UFS) Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 1 module.

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.

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

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Qualcomm® Inline Crypto Engine (UFS) Cryptographic Module 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: SingleChip

Module Characteristics: SubChip

Cryptographic 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 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.

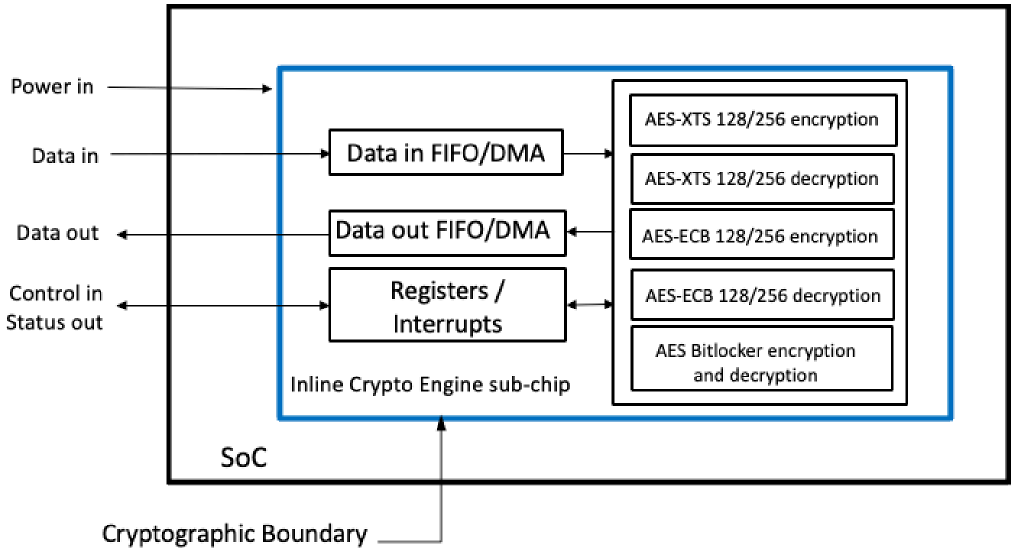

Figure 1: Block Diagram

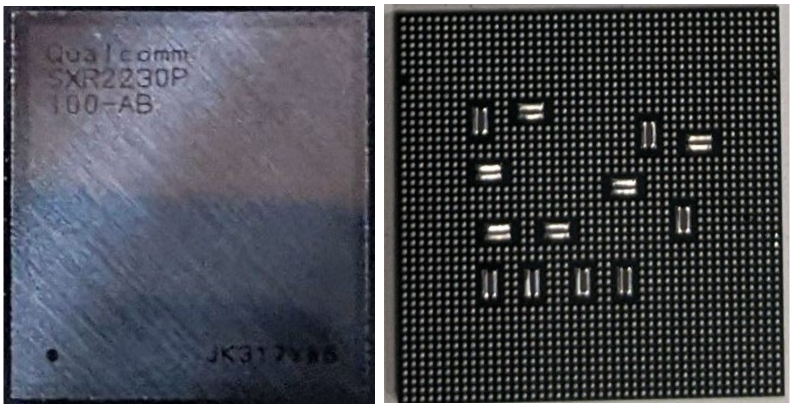

Figure 2: Snapdragon® XR2 Gen 2 Platform

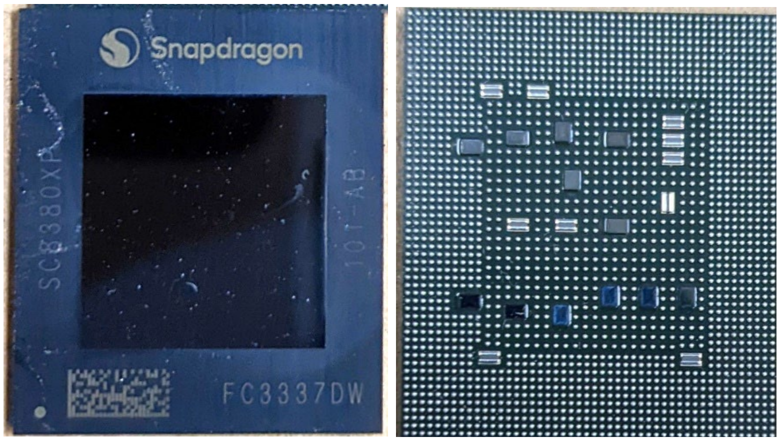

Figure 3: Snapdragon X Elite Compute Platform

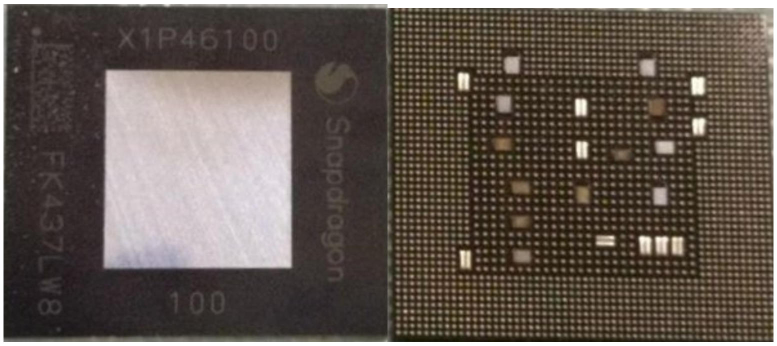

Figure 4: Snapdragon X1 Plus

Tested Operational Environment's Physical Perimeter (TOEPP):

The TOEPP of the module is defined as the entire system-on-chip.

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® XR2 Gen 2 Platform	3.2.1	N/A	Snapdragon® XR2 Gen 2 Platform	N/A
Snapdragon® X Elite Compute Platform	4.0.1	N/A	Snapdragon® X Elite Compute Platform	N/A
Snapdragon® X1 Plus	4.0.1	N/A	Snapdragon® X1 Plus	N/A

Table 2: Tested Module Identification – Hardware

2.3 Excluded Components

There are no components within the cryptographic boundary excluded from the FIPS 140-3 requirements.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service as defined in section 4.3
Non-approved	Automatically entered whenever a non-approved service is requested	Non-Approved	

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 pre-operational 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. 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).

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-XTS Testing Revision 2.0	A2116	Direction - Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A2117	Direction - Decrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A2886	Direction - Encrypt Key Length - 128, 256	SP 800-38E
AES-XTS Testing Revision 2.0	A2887	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 and decryption

Table 5: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AES ECB	BC-UnAuth	AES ECB encryption/decryption	Key size/strength:128 and 256 bits	AES-ECB: (A2117, A2116, A2887, A2886)
AES XTS	BC-UnAuth	AES XTS encryption/decryption	Key size/strength:128 and 256 bits	AES-XTS Testing Revision 2.0: (A2117, A2116, A2887, A2886)

Table 6: Security Function Implementations

2.7 Algorithm Specific Information

AES XTS
The length of a single data unit encrypted or decrypted with AES XTS shall not exceed 2^{20} AES blocks of data per XTS instance. An XTS instance is defined in Section 4 of SP 800-38E.

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.

2.8 RBG and Entropy

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	Data Input	All input data
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	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 (CO)	Role	Crypto Officer	None

Table 8: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AES Encryption	Encryption	"UFS_MEM_ICE_PARAMETERS_4" register bits 0 and 1 indicating value 00	AES Key, plain text	cipher text	AES ECB AES XTS	Crypto Officer (CO) - AES Key: W,E
AES Decryption	Decryption	"UFS_MEM_ICE_PARAMETERS_4" register bits 0 and 1 indicating value 00	AES key, cipher text	plaintext	AES ECB AES XTS	Crypto Officer (CO) - AES Key: W,E
Self-Test	Self-Test is executed automatically when device is booted or restarted	None	N/A	Pass/Fail	None	Crypto Officer (CO)
Show Version	Show the version and name of	None	None	version of module via the UFS_MEM_ICE_VERSION register	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	the module					
Zeroization	Zeroizes all SSps	None	register location of keys	None	None	Crypto Officer (CO) - AES Key: Z
Configuration of parameters for key	Configures the registers to hold parameters such as index of the key	None	Index values for keys	None	None	Crypto Officer (CO)
Show Status	Perform the CASTs	None	None	status via the UFS_MEM_ICE_BIST_STATUS register	None	Crypto Officer (CO)
Setting encryption and decryption keys	Configuring the keys to be used by the module	None	AES Key	None	None	Crypto Officer (CO) - AES Key: W

Table 9: Approved Services

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Bitlocker Encryption	Perform data encryption	AES bitlocker	CO
Bitlocker Decryption	Perform data 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
Opaque enclosure	N/A	N/A

Table 11: Mechanisms and Actions Required

The Qualcomm Inline Crypto Engine (UFS) is a sub-chip enclosed in the platform listed in Table 2 that is 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 registers	Key registers to hold keys	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
Import	calling entity	Hardware registers	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
Module reset	all SSPs are zeroized upon module reset	N/A	N/A

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	AES ECB or XTS key	128 and 256 bits - 128 and 256 bits	CSP - CSP			AES ECB AES XTS

Table 15: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES Key	Import	Hardware registers:Plaintext	Until explicitly zeroized by reset	Module reset	

Table 16: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

N/A for this module.

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.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (A2117)	256 bit key	decryption	CAST	Module becomes operational and services are available for use	Decrypt KAT for ECB	Module initialization
AES-ECB (A2116)	256 bit key	encryption	CAST	Module becomes operational and services are available for use	Encrypt KAT for ECB	Module initialization
AES-ECB (A2886)	256 bit key	encryption	CAST	Module becomes operational and services are available for use	Encrypt KAT for ECB	Module initialization
AES-ECB (A2887)	256 bit key	decryption	CAST	Module becomes operational and services are available for use	Decrypt KAT for ECB	Module initialization

Table 17: Conditional Self-Tests

Self-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 pre-operational 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 (A2117)	decryption	CAST	On demand	Manually
AES-ECB (A2116)	encryption	CAST	On demand	Manually
AES-ECB (A2886)	encryption	CAST	On demand	Manually
AES-ECB (A2887)	decryption	CAST	On demand	Manually

Table 18: Conditional Periodic Information

Periodic self-tests can be invoked by powering-off and reloading the module or when a reset event is received. These tests perform the same pre-operational tests that are performed during power-up. During the execution of the periodic self-tests, cryptographic services are not available, and no data output or input is possible.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Error	This error state is entered if a cryptographic algorithm self-test fails	Known Answer test failure	Module reset	BIST_FAILURE indicator is set

Table 19: Error States

If any of the conditional self-tests or periodic 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 the module is in Error state, 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.

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 defined 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. If one of these verifications fail, 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 section 10 will be executed.

11.2 Administrator Guidance

There is no specific Administrator guidance required for the module.

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, the module does not possess 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.

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