QTI Inline Crypto Engine (UFS)

Version 2.1.0

FIPS 140-2 Non-Proprietary Security Policy

Version 1.2

2016-02-15

Prepared by:

atsec information security corporation

9130 Jollyville Road, Suite 260

Austin, TX 78759

www.atsec.com

TABLE OF CONTENTS

Copyrights and Trademarks

1.Introduction

This document is the non-proprietary FIPS 140-2 Security Policy for the QTI Inline Crypto Engine (UFS) cryptographic module. The version of this cryptographic module is 2.1.0. This document contains a specification of the rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-2 (Federal Information Processing Standards Publication 140-2) for a Security Level 1 hardware cryptographic module.

In this document, the terms “QTI Inline Crypto Engine (UFS)”, “cryptographic module” or “module” are used interchangeably to refer to the QTI Inline Crypto Engine (UFS) cryptographic module.

1.1 Purpose of the Security Policy

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

- it is required for FIPS 140-2 validation,
- it allows individuals and organizations to determine whether the cryptographic module, as implemented, satisfies the stated security policy, and
- it describes the capabilities, protection, and access rights provided by the cryptographic module, allowing individuals and organizations to determine whether it will meet their security requirements.

1.2 Target Audience

This document is part of the package of documents that are submitted for FIPS 140-2 conformance validation of the module. It is intended for the following people:

- Developers working on the release
- FIPS 140-2 testing lab
- Cryptographic Module Validation Program (CMVP)
- Consumers

1.3 Document Organization / Copyright

This non-proprietary security policy document may be reproduced and distributed only in its original entirety without any revision, ©2016 Qualcomm Technologies, Inc.

2.Cryptographic Module Specification

2.1.Description of Module

The QTI Inline Crypto Engine (UFS) is classified as a single chip hardware module for the purpose of FIPS 140-2 validation. It provides XTS-AES encryption and decryption of block storage devices. The logical cryptographic boundary of the module is the QTI Inline Crypto Engine (UFS) 2.1.0, which is a sub-chip hardware component contained within the Qualcomm Snapdragon 820 SoC.

The cryptographic module implements XTS-AES encryption and decryption as defined in SP 800-38E. The underlying AES for XTS-AES is AES ECB compliant to FIPS 197.

The hardware sub-chip cryptographic module is specified in the following table:

Component	Type	Version Number
QTI Inline Crypto Engine (UFS)	Hardware	2.1.0

Table 1: Components of the Hardware Cryptographic Module

The module has been tested on the following platforms:

Qualcomm Snapdragon 820

The module is intended to meet the requirements of FIPS 140-2 at an overall Security Level 1. The table below shows the security level claimed for each of the eleven sections that comprise the validation:

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

Table 2: Security Levels

2.2.Description of Approved Mode

The module supports only FIPS mode.

When the module is powered on, the power-up self-test is executed automatically without any operator intervention. The module enters FIPS mode automatically if the power-up self-test completes successfully.

If any of self-tests fail during power-up, the module goes into Error state. All cryptographic services are prohibited in error state. When an error state is entered the module can be reset to reinitialize the module.

The status of the module can be determined by the availability of the module. If the module is available it has passed all self-tests. If it is unavailable, it is in the error state.

The module 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 module supports a key storage which allows either 2 hardware keys or up to 32 software selectable key contexts. Each context contains one key with one context dedicated to FDE and the remaining to PFE. When an encryption configuration is established, the chosen hardware key or the software selected context key is referenced and will be used for the operation by the module.

The user of this module may also decide not to use the encryption/decryption services provided by this module. Such a decision is not made within the boundary of the module itself. When the user chooses to disable any encryption for write requests and decryption for read requests the module is simply not in use.

The module provides the following CAVP validated algorithm implementations:

Components	Algorithms	Standards	CAVS Certs #
QTI Inline Crypto Engine (UFS)	AES ECB 128/256 (encryption)	FIPS 197	Cert.#: 3557
	AES ECB 128/256 (decryption)	FIPS 197	Cert.#: 3555
	XTS-AES 128/256 (encryption)	SP-800-38E	Cert.#: 3557
	XTS-AES 128/256 (decryption)	SP-800-38E	Cert.#: 3555

Table 3: Approved Algorithms

2.3.Cryptographic Module Boundary

The physical boundary of the module is the physical boundary of the Qualcomm Snapdragon 820 SoC that contains the sub-chip which implements the module. Consequently, the embodiment of the module is a single-chip cryptographic module. The logical boundary of the module is the Inline Crypto Engine sub-chip.

The following figure illustrates the various data, status and control paths through the physical and logical boundary of the cryptographic module.

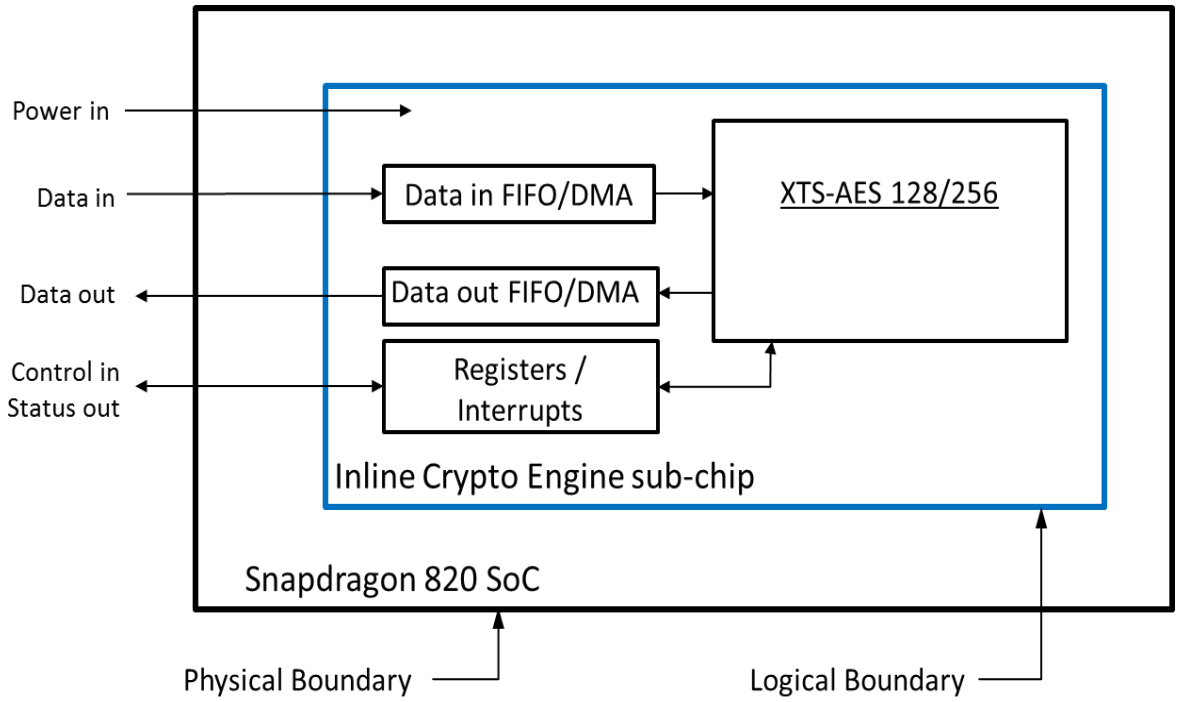
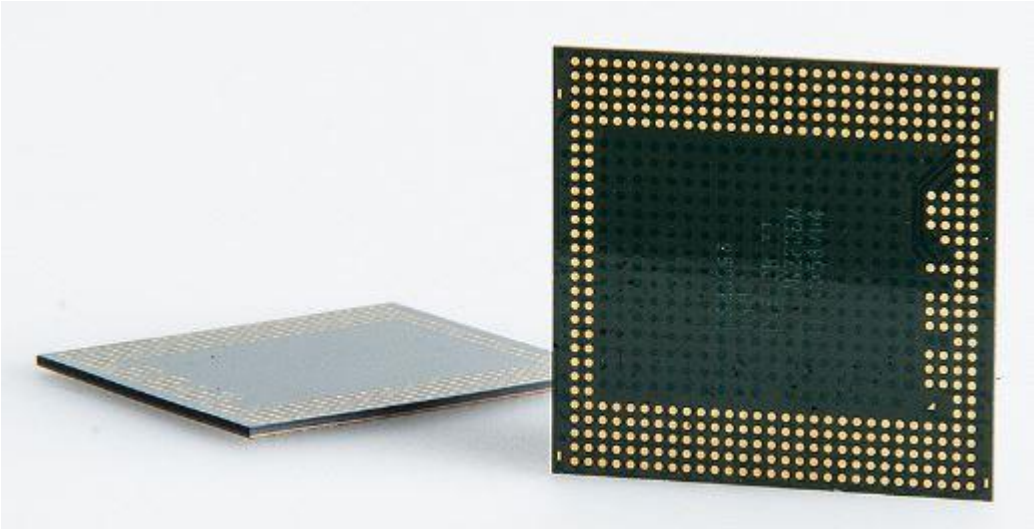
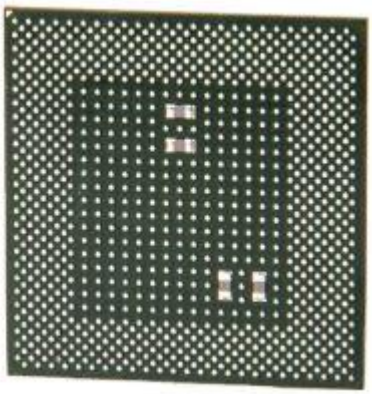


Figure 1: The Physical and Logical Boundary of Inline Crypto Engine (UFS)



Back view



Front view

Figure 2: Qualcomm Snapdragon 820

3.Cryptographic Module Ports and Interfaces

FIPS Interface	Ports
Data Input	Data In FIFO/DMA
Data Output	Data Out FIFO/DMA

FIPS Interface	Ports
Control Input	Registers, Interrupts
Status Output	Registers, Interrupts
Power Input	Physical power connector

Table 4: Ports and Interfaces

4.Roles, Services and Authentication

4.1.Roles

Role	Description
User	Perform general security services, including cryptographic operations; configuration of the module for FDE or PFE.
Crypto Officer (CO)	Configuring the key to be used for the cipher operation.

Table 5: Roles

The module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both User and Crypto Officer roles. The module does not allow concurrent operators.

The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the module. No further authentication is required. The Crypto Officer is responsible to set the key for the cipher operation.

4.2.Services

The module provides XTS-AES-128/256 encryption and decryption. A user may choose whether or not to use the module for its designed services. Once the module is in use, the module does not support a bypass capability to skip the requested encryption or decryption.

The following table describes the services available in FIPS-mode:

Service	Roles		CSP	Access (Read, Write, Execute)
	User	CO		
XTS-AES 128/256 encryption and decryption	✓		Two distinct AES keys	R, W, X
Self-Test (Self-test is executed automatically when device is booted or restarted)	✓		N/A	R, X

Service	Roles		CSP	Access (Read, Write, Execute)
	User	CO		
Zeroization	✓		AES keys	R, W, X
Configuration of operational mode	✓		N/A	R, W
Status output	✓		N/A	R
Setting of encryption keys		✓	N/A	W

Table 6: Services available in FIPS-mode

Note: The methodology for setting the encryption keys is described in the ICE – Inline Crypto Engine Hardware Programming Guide.

4.3.Operator Authentication

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

4.4.Mechanism and Strength of Authentication

No authentication is required at security level 1; authentication is implicit by assumption of the role.

5.Physical Security

The QTI Inline Crypto Engine (UFS) 2.1.0 is a sub-chip module implemented as part of the Qualcomm Snapdragon 820 SoC which is the physical boundary of the sub-chip module. The Qualcomm Snapdragon 820 SoC is a single chip with a production grade enclosure and hence conforms to the Level 1 requirements for physical security.

6.Operational Environment

6.1.Applicability

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

7.Cryptographic Key Management

7.1.Key and CSP List

The only keys/CSPs are the AES keys for XTS-AES encryption and decryption services. These keys are generated outside the module boundary and set up by the Crypto Officer in the registers of the module.

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

Key/CSP	Generation	Storage	Zeroization
AES keys	N/A (Provided by caller, set by Crypto Officer)	Hardware memory (write-only by software)	Zeroized during cold boot of the module

Table 7: Keys and CSPs

7.2.Key/CSP Generation, Entry and Output

The module does not provide any key generation service or perform key generation for any of its Approved algorithms. The caller provides the keys for encryption and/or decryption. Keys are stored in hardware registers (write-only by software) by the Crypto Officer. Once the keys are written to the hardware registers, they are not readable from outside the module.

The cryptographic module does not provide any asymmetrical algorithms or key establishment methods.

7.3.Key/CSP Storage and Zeroization

As stated previously, the CM stores all keys and CSPs internally. All keys and CSPs are stored in on-chip memory (i.e. registers). The key storage memory is able to be read by the CM itself and is write-only (not readable) from outside of the CM. When the module performs a cold boot, it will zeroize all CSPs contained within the module.

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

The CM hardware component cannot be certified by the FCC as it is not a standalone device. It is a sub-chip embedded in the Qualcomm Snapdragon 820 SoC which is also not a standalone device, but rather intended to be used within a COTS device which would undergo standard FCC certification for EMI/EMC.

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

9.Power-Up Tests

Power-Up tests consist of known-answer tests (KAT) of algorithm implementations. The power-up self-tests are automatically performed without any operator intervention during power-up of the module. If any of the power-up self-tests fail, the module will enter the error state. Data output is prohibited and no further cryptographic operation is allowed in the error state. FIPS 140-2 explicitly allows that the on-demand test can be fulfilled with a power cycle of the module. Hence, a power cycle and its associated power-on self-test is the methodology used to perform the "on-demand" tests.

The power-up self-tests are also performed when a module reset event is received. If any of the tests fail, the module will enter an Error state. The module cannot be used in this state. 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.

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

9.1.Cryptographic Algorithm Tests

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

Table 8: Power-Up Cryptographic Algorithm Tests

9.2.Integrity Tests

Not applicable due to module implemented in hardware and is non-modifiable

10.Design Assurance

10.1.Configuration Management

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

11.Mitigation of Other Attacks

No other attacks are mitigated.

12. Glossary and Abbreviations

AES	Advanced Encryption Specification
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
FDE	Full Disk Encryption
FIPS	Federal Information Processing Standards Publication
KAT	Known Answer Test
PFE	Per File Encryption
SoC	System on Chip
UFS	Universal Flash Storage

13.References

[1] FIPS 140-2 Standard,
http://csrc.nist.gov/groups/STM/cmvp/standards.html

[2] FIPS 140-2 Implementation Guidance,
http://csrc.nist.gov/groups/STM/cmvp/standards.html

[3] FIPS 140-2 Derived Test Requirements,
http://csrc.nist.gov/groups/STM/cmvp/standards.html

[4] FIPS 197 Advanced Encryption Standard,
http://csrc.nist.gov/publications/PubsFIPS.html

[5] FIPS 180-4 Secure Hash Standard,
http://csrc.nist.gov/publications/PubsFIPS.html

[6] SP 800-38E Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices,
http://csrc.nist.gov/publications/PubsSPs.html