QTI Crypto Engine Core

Version 5.3.1

FIPS 140-2 Non-Proprietary Security Policy

Version: 1.2

2016-03-11

Prepared for:

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121

Prepared by:

atsec information security Corp.
9130 Jollyville Road, Suite 260
Austin, TX 78759

Table of Contents

Copyrights and Trademarks

1. Introduction

This document is a FIPS 140-2 Security Policy for the QTI Crypto Engine Core cryptographic module. The version number of this cryptographic module is 5.3.1. 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 Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2) for a Security Level 2 module. It is intended for the FIPS 140-2 testing lab, Cryptographic Module Validation Program (CMVP), developers working on the release, administrators of the cryptographic module and users of the cryptographic module.

For more information about the FIPS 140-2 standard and validation program, refer to the NIST website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

In this document, the terms “QTI Crypto Engine Core”, “cryptographic module” “CM” or “the module” are used interchangeably to refer to the QTI Crypto Engine Core Cryptographic Module.

1.1.Purpose of the Security Policy

There are three major reasons that a security policy is required

- It is required for FIPS 140-2 validation.
- It allows individuals and organizations to determine whether the implemented cryptographic module satisfies the stated security policy.
- It allows individuals and organizations to determine whether the described capabilities, the level of protection, and access rights provided by the cryptographic module meet their security requirements.

2. Cryptographic Module Specification

2.1.Module description

The Cryptographic Module (CM) is a single-chip hardware module implemented as a sub-chip in the Qualcomm Snapdragon 820 SoC. From the validation perspective the CM is configured as a single chip hardware module. The cryptographic services provided by the module are:

- Data encryption / decryption utilizing symmetric ciphers, i.*e.* Triple-DES, and AES algorithms.
- Computation of hash values, i.*e.* SHA-1, SHA-256.
- Message authentication utilizing HMAC-SHA1, HMAC-SHA256, AES CMAC, hashing algorithms.
- Hashing and ciphering operations using AES CCM.

Table 2-1: Summary of FIPS approved and FIPS non-approved algorithms in the CM

FIPS Approved	Implemented Algorithms
AES-128 CBC, AES-256 CBC	encryption, decryption
AES-128 ECB, AES-256 ECB	encryption, decryption
AES-128 CTR, AES-256 CTR	encryption, decryption
AES-128 CCM, AES-256 CCM	encryption, decryption (with message authentication code)
AES-128 XTS, AES-256 XTS[1]	encryption, decryption
Triple-DES CBC (three-key)	encryption, decryption
Triple-DES ECB (three-key)	encryption, decryption
SHA-1	Hashing
SHA256	Hashing
HMAC SHA-1 with key sizes between 112 bits and 512 bits	message authentication code
HMAC SHA-256 with key sizes between 112 bits and 512 bits	message authentication code
AES-CMAC	message authentication code
FIPS Non-Approved	**Implemented Algorithms**
DES CBC	encryption, decryption
DES ECB	encryption, decryption
HMAC SHA-1 with key sizes below 112 bits	message authentication code
HMAC SHA-256 with key sizes below 112 bits	message authentication code
AEAD-SHA-1 AES CBC	encryption, decryption (with message authentication code)
AEAD-SHA-1 AES CTR	encryption, decryption (with message authentication code)
AEAD-SHA-1 DES CBC	encryption, decryption (with message authentication code)
AEAD-SHA-1 Triple-DES CBC	encryption, decryption (with message authentication code)

[1] AES-XTS mode is only approved for storage applications

1. Caveat: AES counter mode uses a 128 bit counter. The counter will roll over after 2^128 blocks of encrypted data.

2.1.1.Hardware description

The cryptographic module is implemented in the QTI Crypto Engine Core 5.3.1 hardware, which resides in Qualcomm Snapdragon 820 processors (https://www.qualcomm.com/products/snapdragon/processors/820). The QTI Crypto Engine Core 5.3.1 provides a series of algorithms (as listed in Table 2-1) implemented in the device hardware.

2.1.2.Module Validation Level

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

Table 2-2: Security Levels

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				

The QTI Crypto Engine Core is classified as a single-chip hardware module for the purpose of FIPS 140-2 validation. The logical cryptographic boundary for the module is the sub-chip implementing the module while the physical boundary is the Qualcomm Snapdragon 820 SoC.

The module was tested as a sub-chip implemented within the Qualcomm Snapdragon 820 SoC.

2.2.Description of Modes of Operations

The CM supports a FIPS approved mode and a non-approved mode. All CSPs are kept separate between the two modes. The services available in each mode are specified in Table 4-2. When a request for a non-approved mode service is received, the CM switches to non-approved mode, services the request, and immediately switches back to the approved mode.

The CM is placed into the approved mode by performing power up self-tests consisting of a KAT self-test for each algorithm available in the approved mode. If any test fails, none of the cryptographic functions are available.

Table 2-1 provides a summary of all security functions (both FIPS Approved and FIPS non-Approved). Table 4-1 lists the roles and Table 4-2 along with table 4-3 illustrates the services available to each role (Crypto Officer and User).

2.3.Cryptographic Module Boundary

The physical boundary of the module is the physical boundary of the Qualcomm Snapdragon 820 SoC which contains the module which is implemented as a sub-chip. Consequently, the embodiment of the module is a Single-chip cryptographic module. The logical boundary of the module is the QTI Crypto Engine Core.

2.3.1.Hardware Block Diagram

In the hardware block diagram, the arrows depict the flow of the status, control and data. Parameters are passed to the module and results received from the module via Direct Memory Access (DMA) writing and reading the modules registers.

The CSPs, such as the encryption key, are written directly to registers or submitted via the FIFO channel to be stored within the QTI Crypto Engine Core 5.3.1 hardware. The remainder of the Qualcomm Snapdragon 820 SoC, which is not part of the QTI Crypto Engine Core, either passes the Critical Security Parameters (CSP) from the software executing on top of the SoC to the QTI Crypto Engine Core, or as a “user” of cryptographic services generates the CSP and delivers them to the QTI Crypto Engine Core.

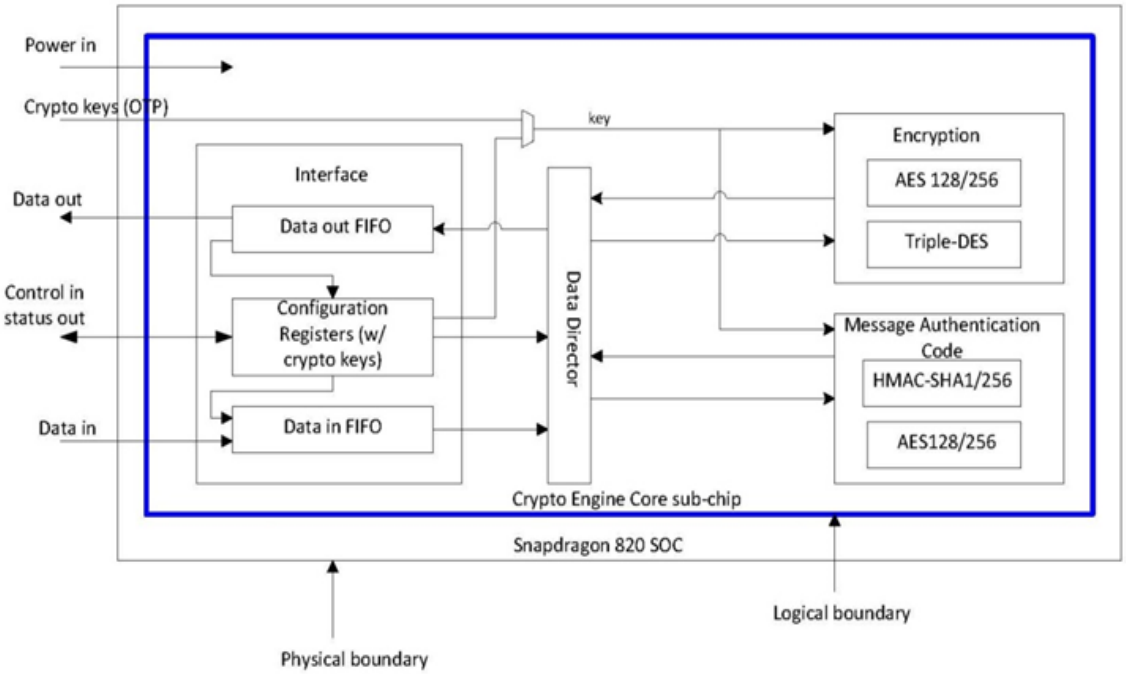
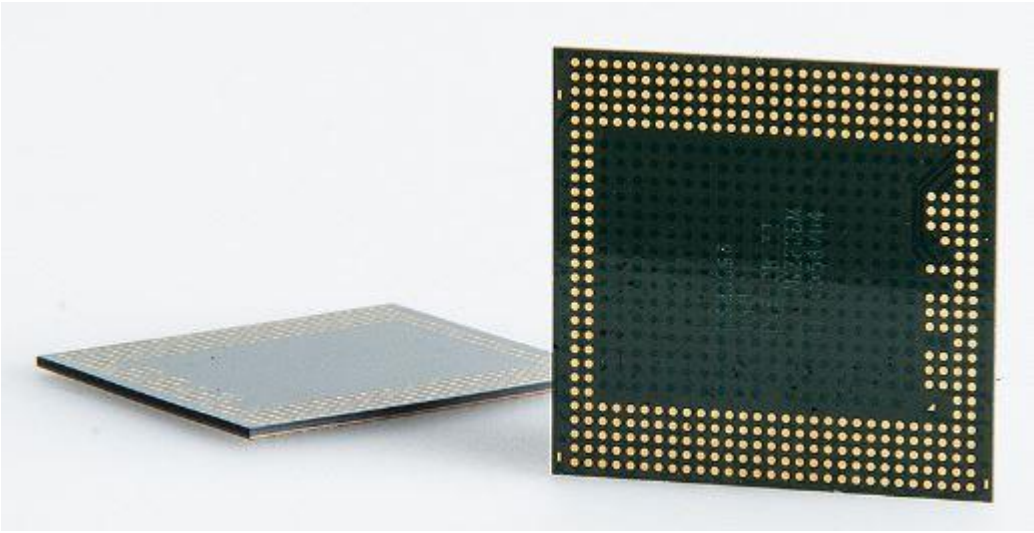


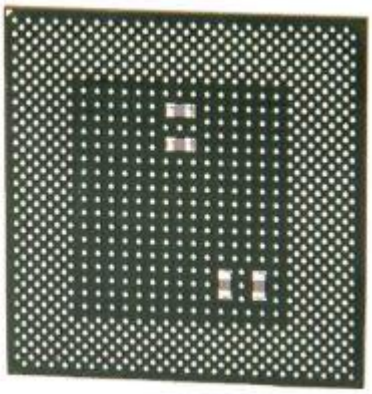
Figure 1: Hardware Block Diagram

The CSPs are passed via Direct Memory Access (DMA) to first In first out queues (FIFOs) and processed by the Cryptographic Module. All parameters to the module are also provided via FIFOs.

Figure 2: Qualcomm Snapdragon 820 processor



Back view



Front view

3.Cryptographic Module Ports and Interfaces

Table 3-1 Ports and interfaces

FIPS Interface	Ports
Data Input	Data in FIFOs
Data Output	Data out FIFOs
Control Input	Registers
Status Output	Registers
Power Input	Physical power connector

As indicated in Table 3-1, all status ports and control ports are directed through the interface of the module's logical boundary, which is the registers of the module for control input. For data input and data output, the FIFOs implement the high-speed interface. The status output is provided via registers.

Once the module finishes initialization and all self-tests complete successfully, all cryptographic functions are made available. If any of the module's KAT fails, the module self-test causes the module to enter a locked state (see Section 9.1 for more details). To recover from a KAT failure a reset of the module is required which causes it to reinitialize and re-run all KATs.

Caller-induced or internal errors do not reveal any sensitive material to callers. Cryptographic bypass capability is not supported by the module. The CM ensures that there is no means to obtain CSP or key data from the cryptographic module by placing the CSPs into write-only registers preventing any entity interacting with the module from being able to read the CSPs. Additionally, key zeroization can be performed by issuing a reset event to the module. There is no means to obtain sensitive information from the cryptographic module.

If a caller wants to use a non-Approved cipher, a separate "pipe pair" must be used or a new key for the non-Approved cipher must be loaded.

4.Roles, Services and Authentication

4.1.Roles

The module supports two roles: a Crypto Officer role and a User role. Roles are implicitly assumed based on the services requested.

Users of the module are the boot loader and software applications loaded onto the Qualcomm Snapdragon 820 SoC. In a typical use case scenario of the module, an Original Equipment Manufacturer (OEM) places a hash of their RSA public key into the One-Time Programmable (OTP) memory within the cryptographic module upon the purchase of Qualcomm Snapdragon 820 SoC. The OEM uses the uniquely matching private key to sign the boot loader and software application images along with the software IDs. The OEM also includes a copy of the OEM's x.509 certificate in each signed image.

The user authentication is based on RSA signature verification and is explained in more detail in the following sections.

4.1.1.Crypto Officer Role

The boot loader assumes the Crypto Officer role when it initializes the module by properly setting up keys/CSPs in the designated key registers or the FIFOs that will be later used by the software applications.

4.1.2.User Role

The software applications assume the User role when requesting any services provided by the module. The User role has access to all of the module's services except module initialization.

Table 4-1 Roles

Role	Services (see Table 4-2 and 4-3)
User	Utilization of cryptographic services of the module
Crypto Officer	Initialize module keys for use by user role

4.2.Services

The crypto module does not provide a bypass capability through which some cryptographic operations are not performed or where certain controls implemented during normal operation are not enforced.

All services are implemented within the hardware module.

The following tables (Table 4-2 and Table 4-3) illustrate the role and corresponding services of the Crypto Officer and User.

Table 4-2 Approved Services

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write, Execute)	Standard
	User	CO					
Symmetric Algorithms							
AES encryption and decryption	✓		AES Symmetric key (128, 256 bit)	CBC, ECB, CTR, XTS[2], CCM	Cert. 3526	Read/Write	FIPS 197 SP 800-38 [A,C,E]
Triple-DES	✓		Triple DES Symmetric key (192 bits)	CBC, ECB	Cert. 1980	Read/Write	FIPS 46-3 SP 800-38A
Hash Functions							
SHA-1	✓		None	N/A	Cert. 2909	Read/Write	FIPS 180-4
SHA-256	✓		None	N/A	Cert. 2909	Read/Write	FIPS 180-4
Message Authentication Codes (MACs)							
HMAC SHA-1	✓		HMAC SHA-1 key (key length between 112 bits and 512 bits)	N/A	Cert. 2254	Read/Write	FIPS 198-1
HMAC SHA-256	✓		HMAC SHA-256 (key length between 112 bits and 512 bits)	N/A	Cert. 2254	Read/Write	FIPS 198-1
AES-CMAC	✓		AES Symmetric key (128, 256 bit)	CMAC	Cert. 3526	Read/Write	SP 800-38B
Miscellaneous							
Initialize module keys for use by User role[3]		✓	None	N/A	N/A	Read/Write	N/A

[2] AES-XTS mode is only approved for storage applications.

[3] The methodology for setting the encryption keys is described in the “Crypto Core Hardware Programming Guide” manual

Service	Roles		CSP	Modes	Is FIPS Approved? If Yes Cert #	Access (Read, Write, Execute)	Standard
	User	CO					
Self Tests	✓		None	N/A	N/A	Execute	N/A
Zeroization	✓		All CSPs	N/A	N/A	N/A	N/A
Query status	✓		None	N/A	N/A	Read	N/A

Table 4-3 Non-Approved Services

Service	Roles		Access (Read, Write, Execute)
	User	CO	
Symmetric Algorithms			
DES	✓		Read/Write
HMAC SHA-1 with key size less than 112 bits	✓		Read/Write
HMAC SHA-256 with key size less than 112 bits	✓		Read/Write
AEAD-SHA-1 AES	✓		Read/Write
AEAD-SHA-1 DES	✓		Read/Write
AEAD-SHA-1 Triple-DES	✓		Read/Write

4.3.Identification and Authentication

As mentioned previously, user authentication is based on RSA signatures. Each OEM utilizes their unique RSA private key to sign the boot loader and software application images along with its x.509 certificate. The x.509 certificate contains the OEM's public key. The OU field (i.e. the field indicating the Certification Services Division) of the signed x.509 certificate contains the software

ID. Finally, the OEM puts a hash of its public key into non-volatile read-only OTP memory within the module.

The user is identified via the software ID embedded in the loadable image. The user authentication performed is twofold. First, the OEM's public key in the x.509 certificate within the image is hashed and the hash value is compared to the hash of the RSA public key stored in read-only memory within the module. If the hashes match, the OEM's public key is verified. Then, the OEM's public key is used to verify the RSA signature of the boot loader or the software image to be loaded. If the RSA signature verification succeeds, then the image is authenticated and hence can be loaded and executed on the Qualcomm Snapdragon 820 SoC.

4.4.Strength of Authentication

Storing a hash of the OEM's public key within the modules read-only memory allows the OEM to choose the size of the RSA key they want to use for authentication to the module. The minimum RSA key size that an OEM may use is 2048-bits. According to table 4 in FIPS IG 7.5, an RSA key size of 2048 bits provides a minimum of 112 bits of strength and a key size of 3072 bits provides a minimum of 128 bits of strength. Therefore, the strength of the authentication mechanism in use is a minimum of $1 / 2^{112}$ or 1.925929944e-34. The ability to successfully authenticate the RSA signed image is dependent on the ability to guess the signing RSA private key that matches the verified public key. Even using a rate of 1µs per failed authentication, which would allow 60,000,000 consecutive attempts per minute (60s / 0.001s), only provides a probability of successfully authenticating that is less than or equal to $60,000,000 * 1 / 2^{112}$ (≤6.933347799e-19) which is much less than 1 / 100,000 or 0.00001.

4.5.Authentication Data Protection

The hash of the RSA public key stored in the read-only memory of the module is used as the means to verify the OEM's public key. Since this memory is non-volatile read-only memory it cannot be modified. The verified public key is used to verify the OEM's RSA signature of the signed boot loader or software application images. Only the images that are signed by the OEM can be authenticated to the module. Any image with an altered RSA signature won't be authenticated and hence won't be loaded and get to use the module.

5.Physical Security

5.1.Type

The QTI Crypto Engine Core Cryptographic Module is a hardware module that operates on a single-chip standalone platform which conforms to the Level 2 requirements for physical security. The cryptographic module is a sub-chip enclosed in a production grade component.

At the time of manufacturing the die is embedded within a printed circuit board (PCB) which prevents visibility into the internal circuity of the module. 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 CM 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 completely surrounds the CM.

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/CSP Generation Management

The module does not perform key generation for any of its approved algorithms or other algorithm.

The CM does not provide any asymmetric algorithms. Manual key entry or key output capabilities are not provided. All Keys/CSPs can only be written to the CM by the boot loader by writing to the key registers or into the FIFOs assigned to the particular use case.

Callers pass keys and similar sensitive information to the CM by writing to specific assigned registers by sending the data via DMA request. Any attempt to write to a non-assigned FIFO is blocked. Keys are stored within the CM in write-only registers or the module's internal key store, therefore any attempt to read CSPs are blocked and zeros are returned rather than the actual CSP.

Keys and CSPs can be explicitly zeroized by sending an access control reset event to the module.

7.2.Zeroization

As stated previously, the CM stores all keys and CSPs internally. All keys and CSPs are stored write-only and are not readable outside of the CM. When the module receives a reset event it will zeroize all CSPs contained within the module.

7.3.Key/CSP Lifecycle

The following table shows the generation, storage and zeroization of all CSPs used by the module.

Table 7-1 Key/CSP Lifecycle

Key/CSP	Generation	Storage	Zeroization
AES Keys	N/A	Internal key storage memory or Register set (legacy use)	During module reset or when overwritten by new key
Triple-DES Keys	N/A	Internal key storage memory or Register set (legacy use)	During module reset or when overwritten by new key
HMAC Keys	N/A	Internal key storage memory or Register set (legacy use)	During module reset or when overwritten by new key
CMAC Keys	N/A	Internal key storage memory or Register set (legacy use)	During module reset or when overwritten by new key

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 imbedded 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 self-tests consist of known-answer tests of algorithm implementations. The module power up tests are automatically performed independent of any user during power up of the module. All self-tests are performed as a single atomic action that has two possible results: success or failure. If the result is success, the CM becomes operational, if it is failure, the CM enters an error state and cryptographic functions cannot be performed.

The power up tests are also run 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 tests trigger immediately when a reset occurs and execute all needed tests until completion. Once completed successfully, the logic releases the module for external usage. If an error is detected during the tests, the 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.

“On demand” tests which are required by FIPS 140-2 can be performed by either of the following methods:

- A power-off/power-on cycle of the module
- Issuing a Crypto Core reset to the module

The CM implements the following self-tests to ensure proper functioning of the module Implemented self-tests include power up self-tests of all approved algorithms.

9.1.Cryptographic algorithm tests (known answer tests)

Table 9-2 Power up Tests

Algorithm	**Test**
AES encryption (CCM)	KAT
AES decryption (CCM)	KAT
AES encryption (ECB)	KAT
AES decryption (ECB)	KAT
Triple-DES encryption (ECB)	KAT
Triple-DES decryption (ECB)	KAT
HMAC SHA-1	KAT
HMAC SHA-256	KAT
AES-CMAC	KAT

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.

10.1.1.Crypto Officer Guidance

The cryptographic module does not need FIPS 140-2 specific guidance. The FIPS 140-2 functional requirements are always invoked.

For configuring the identification mechanism as well as the access control functionality, the manual for the QTI Crypto Engine Core should be used.

11. User Guidance

The operation of the cryptographic module does not need FIPS 140-2 specific guidance. The FIPS 140-2 functional requirements are always invoked.

For using the cryptographic services of the module, the manual for the QTI Crypto Engine Core covering the description of the register set as well as the use of the FIFOs channels should be used.

12. Mitigation of Other Attacks

The Mitigation of Other Attacks security section of FIPS 140-2 is not applicable to the QTI Crypto Engine Core.

13.Terms and Abbreviations

AES	Advanced Encryption Specification
CBC	Cipher Block Chaining
CCM	Counter with Cipher Block Chaining-Message Authentication Code
CM	Cryptographic Module
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off The Shelf
CO	Crypto Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
DMA	Direct Memory Access
FIFO	First In, First Out
FIPS	Federal Information Processing Standards Publication
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
NIST	National Institute of Science and Technology
OEM	Original Equipment Manufacturer
OTP	One-Time Programmable
QTI	Qualcomm Technologies, Inc.
SHA	Secure Hash Algorithm
SoC	System on Chip