FIPS 140-2 Non-Proprietary Security Policy

AWS Nitro Card Security Engine

(Hardware version AL5+, firmware version HAL-rel-3.2-uemu-fips)

Document Version 1.03.00

October 22, 2020

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards (FIPS) Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140-2 program. The National Voluntary Laboratory Accreditation Program (NVLAP) accredits independent testing labs to perform FIPS 140-2 testing; the CMVP validates modules meeting FIPS 140-2 validation. *Validated* is the term given to a module that is documented and tested against the FIPS 140-2 criteria.

More information is available on the CMVP website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the AWS Nitro Card Security Engine from Amazon Web Services (AWS) provides an overview of the Security Engine and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

In this document, the terms "AWS Nitro Card Security Engine", "cryptographic module", "AWS Cryptographic Module", "CM" or "the module" are used interchangeably to refer to the AWS Nitro Card Security Engine.

1.3 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.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

Table 1- Acronyms and Terms defines acronyms found in this document:

Acronym	Term
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
AWS	Amazon Web Services
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSE	Communications Security Establishment Canada
CSP	Critical Security Parameter
EBC	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	(Keyed-) Hash Message Authentication Code
KAT	Known Answer Test
MAC	Message Authentication Code
MD	Message Digest
NIST	National Institute of Standards and Technology
SHA	Secure Hash Algorithm
SP	Special Publication

Table 1- Acronyms and Terms

2 AWS Nitro Card Security Engine

2.1 Cryptographic Module Specification

The Cryptographic Module (CM) is a multi-chip standalone firmware-hybrid module. The cryptographic services available in the module's Approved mode of operation are as follows:

- Data encryption / decryption utilizing symmetric ciphers, i.e. AES algorithms.
- Computation of hash values, i.e. SHA-256, SHA-512.
- Message authentication utilizing HMAC-SHA256 and HMAC-SHA512 message authentication algorithms.

The module's cryptographic algorithm implementations have received the following certificate numbers from the Cryptographic Algorithm Validation Program (CAVP).

CAVP Cert.	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
C997	**AES**	FIPS 197	ECB	128, 256	Encryption, Decryption
C997	**XTS**[1]	SP 800-38E	AES	128, 256	Encryption, Decryption
C997[2]	**SHS**	FIPS 180-4	SHA-256, SHA-512	--	Hashing
C2168	**HMAC**	FIPS 198-1	SHA-256, SHA-512	256, 512	Message Authentication Code

Table 2-Summary of FIPS algorithms in CM

Additionally, the module supports the following algorithms in the non-Approved mode of operation:

- DES-ECB
- DES-CBC
- 3DES-ECB
- 3DES-CBC
- AES-ECB-192
- AES-XTS-192
- AES-CBC-128, AES-CBC-192, AES-CBC-256
- AES-CTR-128, AES-CTR-192, AES-CTR-256
- AES-CCM-128, AES-CCM-192, AES-CCM-256

[1] The XTS mode of encryption is only intended for use with storage applications.
[2] The module does not implement all functions tested via CAVP.

- AES-GCM-128, AES-GCM-192, AES-GCM-256
- MD5
- SHA1
- SHA2-384
- SHA3-224, SHA3-256, SHA3-384, SHA3-512
- SHA3-def
- SHAKE128
- SHAKE256
- HMAC-SHA1
- HMAC-SHA2-384
- HMAC-SHA3-224, HMAC-SHA3-256, HMAC-SHA3-384, HMAC-SHA3-512

2.1.1 Hardware Description

The hardware portion of the cryptographic module is the AL5+ System-on-a-chip (SoC), which provides AES-ECB, AES-XTS, and SHA algorithm implementations.

2.1.2 Firmware Description

The firmware portion of the cryptographic module consists of the C-based HAL (Hardware Abstraction Layer) firmware components executed by the Cortex ARMv8 processor as well as the HMAC integrity check files as follows:

- libalfips.so
- alfips.hmac

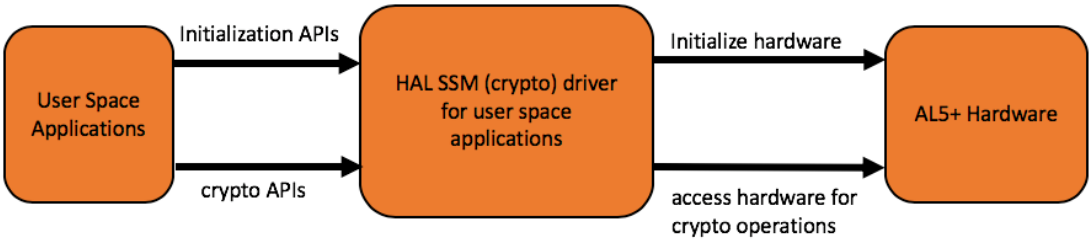

Figure 1-Cryptographic modules depicting the driver modules to access the AL5+ hardware

In addition, the firmware portion of the module implements the HMAC algorithm leveraging the underlying SHA implementation in the AL5+ hardware.

2.1.3 Module Validation Level

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

Table 3-Validation Level by FIPS 140-2 Section lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
Electromagnetic Interference / Electromagnetic Compatibility	1
Self-Tests	1
Design Assurance	1
Mitigation of Other Attacks	N/A
Overall Level	**1**

Table 3-Validation Level by FIPS 140-2 Section

Table 4 describes the platform where the cryptographic module has been tested:

Module Name	Hardware Version	Firmware Version	OS
AWS Nitro Card Security Engine	AL5+	HAL-rel-3.2-uemu-fips	Carbon Linux

Table 4-Tested Platforms

2.2 Description of Approved Modes

The CM supports an Approved mode and a non-Approved mode. The Approved and non-Approved services available are specified in section 4.2. There is no sharing of CSPs between Approved and non-Approved modes.

The CM is placed into the approved mode by performing power up self-tests consisting of a KAT self-test for each algorithm in the approved list and a firmware integrity test. If either test fails, the module enters an error state, returns an error code to the calling application and inhibits all data output.

Table 7 illustrates the role and corresponding services available to the Crypto officer and User.

2.3 Cryptographic Module Boundary

The physical boundary of the module is the physical boundary of the AL5+ chip. Consequently, the embodiment of the module is a Multi-chip standalone cryptographic module.

In the following diagram, the bidirectional arrows depict the flow of the status, control and data. The logical boundary of the cryptographic module contains only the user space library and the AL5+ hardware.

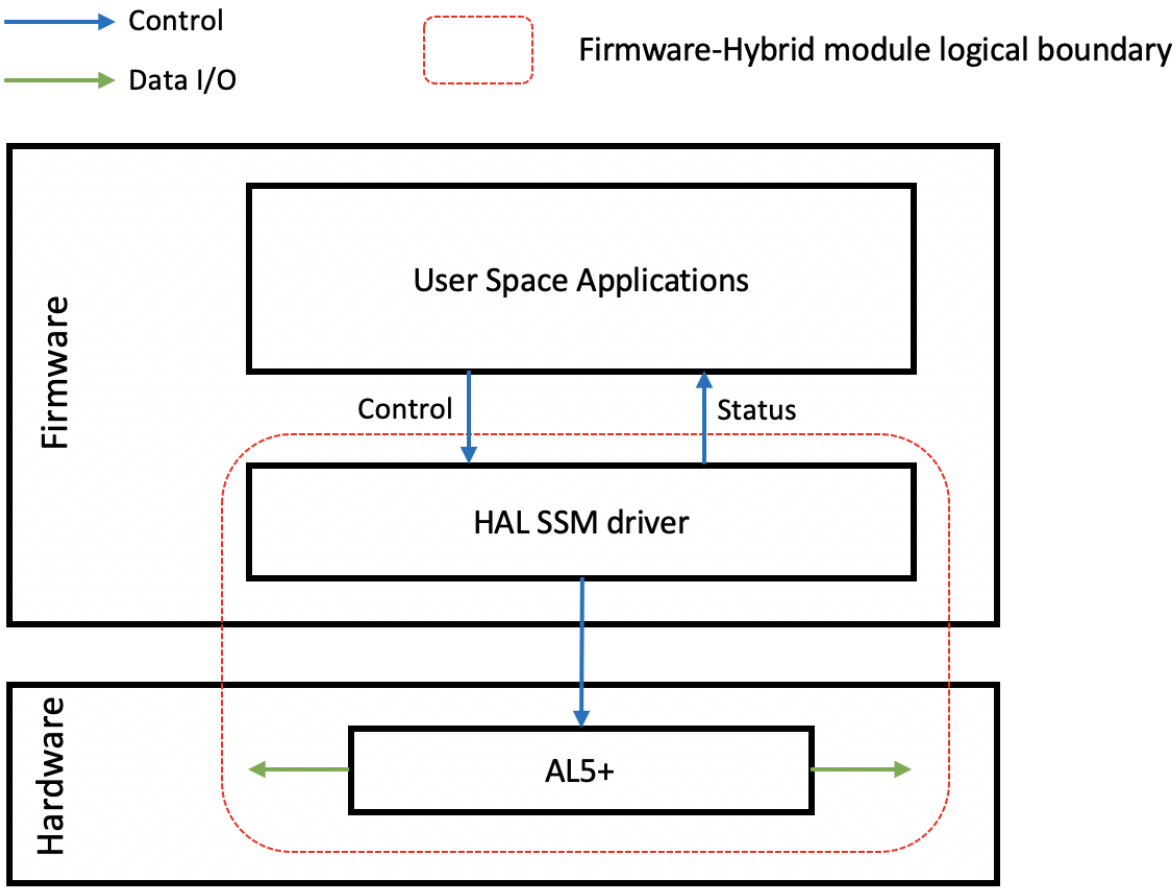

Figure 2-Cryptographic Boundary

The operations within the logical security boundary use the ciphers from the AL5+ hardware (see Figure 3) that is included in the logical boundary.

2.3.1 Hardware Block Diagram

Figure 3 and Figure 4 below depict a hardware block diagram and hi-resolution photos of the module. In the block diagram, the bidirectional arrows depict the flow of the status, control and data. Firmware drivers pass the parameters to the hardware and receive the results from the hardware.

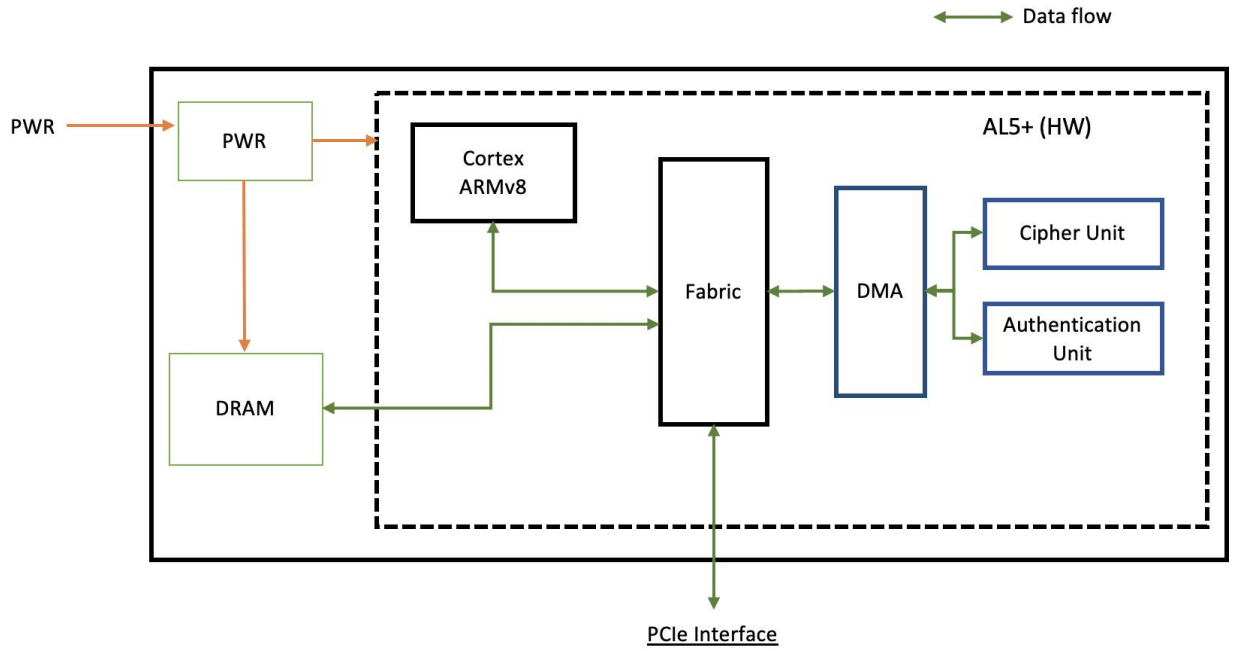

Figure 3-Hardware Block Diagram

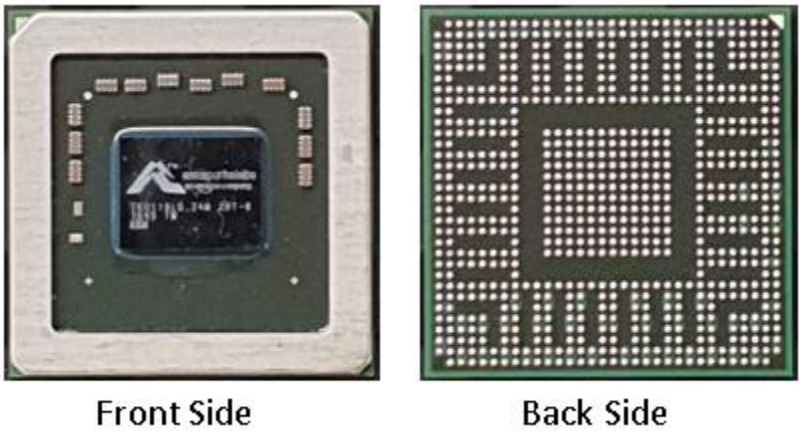

Figure 4-AL5+ Hi-resolution photos

3 Cryptographic Module Ports and Interfaces

FIPS Interfaces	Ports
Data Input	API input parameters
Data Output	API output parameters
Control Input	API function calls
Status Output	API return codes, log messages

Table 5-Ports and interfaces

As indicated in Table 5, all status ports and control ports are directed through the interface of the module's logical boundary, which is the software APIs of the module.

The User or Crypto Officer interacts with the CM in two distinct ways:

- Powering on the CM
- The application services (API's) invoked by user space applications

Once the user space applications initialize the cryptographic module and the self-tests complete successfully, all cryptographic functions are made available to user space. If any of the modules KAT fails, the module self-test causes the system to panic (see Section 9.1 for more details). To recover from a KAT failure a reboot of the hardware is required to reset the failure status. If the integrity tests fail the module causes assert, thereby shutting down the applications and HAL SSM (crypto) driver and the CM. The only way to recover from an integrity test failure is to reboot the hardware and restart HAL SSM (crypto) driver.

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 data from the cryptographic module by performing key zeroization at the completion of each service. There are no means to obtain sensitive information (including CSPs) from the cryptographic module.

4 Roles, Services and Authentication

4.1 Roles

The module supports two roles: a Crypto Officer role and a User role. The module does not support user identification or authentication that would allow the module to distinguish between the two supported roles.

The Crypto Officer role is a purely administrative role that does not involve the use of cryptographic services. The role is not explicitly authenticated but assumed implicitly on implementation of the module's installation and initialization.

The User role has access to all the module's services. The role is not explicitly authenticated but assumed implicitly on access of any of the non-Crypto Officer services. An operator is implicitly in the User or Crypto Officer role based upon the service chosen. If any of the User-specific services are called, then the operator is in the User role; otherwise the operator is in the Crypto Officer role.

The customer who configures and installs the CM is considered to be a Crypto Officer. Additionally, a user powering up and initializing the device is assuming the Crypto Officer role. There is no enforced separation between the Crypto Officer and the User roles. As stated previously, the User or Crypto Officer role is based on the service or operation performed.

Role	Services (see Table 4-2)
User	Utilization of services of the module
Crypto Officer	Installation and Initialization of the module

Table 6-Roles

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.

Services and sub-services are split between the software and hardware portions of the firmware hybrid module as follows:

- ciphers: hardware where the software driver is used for proper alignment of data and invocation of hardware
- selftest / integrity test: firmware

The following table (Table 7-Approved Services) illustrates the role and corresponding services of the Crypto Officer and User. Additionally, the Component column "C" indicates the component that implements the service with 'H' indicating hardware, 'F' indicating firmware and "H/F" indicating hardware and firmware.

Services	User	CO	C	CSP	Modes	Access Type
AES-ECB encryption and decryption	✓		H	AES Symmetric key (128,256 bit)	ECB	Read/Write/Execute/Zeroize
AES-XTS encryption and decryption	✓		H	AES Symmetric Key (128,256 bit)	XTS	Read/Write/Execute/Zeroize
SHA2-256	✓		H	None	N/A	N/A
SHA2-512	✓		H	None	N/A	N/A
HMAC-SHA2-256	✓		H/F	HMAC-SHA256 key with a length of at least 112 bits	N/A	Read/Write/Execute/Zeroize
HMAC-SHA2-512	✓		H/F	HMAC-SHA512 key with a length of at least 112 bits	N/A	Read/Write/Execute/Zeroize
Module installation		✓	N/A	None	N/A	N/A
Self-Tests	✓		F	HMAC-SHA-256 key for integrity test	N/A	N/A
Zeroization	✓		F	All CSPs	N/A	Zeroize
Query Status	✓		F	None	N/A	N/A

Table 7-Approved Services

The module supports a set of services in the non-Approved mode of operation, which are a 1 to 1 mapping of the non-Approved algorithms as specified in section 2.1 above.

5 Physical Security

The Cryptographic Module is a firmware-hybrid module that operates on a multi-chip standalone platform which conforms to the Level 1 requirements for physical security. The hardware portion of the cryptographic module is a production grade component. The device using the CM shall be comprised of production grade components with standard passivation (a sealing coat applied over the chip circuitry to protect it against environmental and other physical damage) and a production grade enclosure that completely surrounds the cryptographic module.

6 Operational Environment

The module's operational environment is non-modifiable and is comprised of Carbon Linux running on the AL5+ SoC.

7 Cryptographic Key Management

The following keys, cryptographic key components and other critical security parameters are contained in the module:

Keys/ CSPs	Storage	Generation/Input	Zeroization Method
HMAC Key	DRAM (Plaintext)	The Key is passed into the module via API input parameter.	The calling application is responsible for calling the appropriate zeroization function from the available APIs
AES XTS (K1 and K2)			
AES XTS IV			
Generic AES Key			

Table 8-Keys and CSPs

7.1 Key/CSP Generation Management

The module does not perform key generation for any of its approved algorithms. Keys are passed in from user space applications via algorithm APIs.

The CM does not provide any key generation algorithms. Manual key entry or output capabilities are not supported. Any CSP references can only be exchanged between the CM and the calling application through the appropriate API calls. The CSPs, such as the encryption key, are given to the APIs via DMA descriptors. All API calls occur within the physical boundary of the device.

Application pass references to keys and similar sensitive information to the CM using API calls. It is the applications responsibility to destroy this information using FIPS Pub 140-2 compliant procedures. The CM itself does not destroy externally stored keys and secrets since it does not own these CSPs. Keys are not stored within the CM; however intermediate key material may reside in memory as clear data. All intermediate key storage and other CSPs stored or created by the CM are zeroized when processing completes.

7.2 Zeroization

Services can be called by the application running in the user space. When the service is called by the application running in the user mode, user level HAL SSM (crypto) driver performs the zeroization operation by accessing hardware. No kernel mode is involved in this process.

8 Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC)

The CM was tested for EMI/EMC and found to be compliant with FCC Part 15 subpart B (Class A digital device).

9 Powerup Tests

Powerup self-tests consist of software integrity tests and known-answer tests of algorithm implementations. The module integrity test is automatically performed during loading. If any of these tests fail, the module will terminate the loading process. The module cannot be used in this state. To recover from the error state, re-initialization is possible by doing a reboot to set it to power on state.

Powerup self-tests are performed when the CM is initialized. Initialization is invoked by an application that is human user independent. 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. 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.

If any of the tests fail, the module will cause the system to panic and all functionality to stop. All cryptographic requests other than those made by the integrity test module are blocked during the integrity test. The integrity test uses cryptographic functions in the CM to perform the integrity test. If the integrity test of any component fails, all the services are blocked, and no crypto operations are available. If the test passes the CM will unblock the cryptographic requests. This causes the CM to enter FIPS operational mode.

9.1 Self-tests

The CM implements self-tests to ensure proper functioning of the module. Implemented self-tests include powerup self-tests and conditional self-tests. The powerup self-tests include known answer tests (KAT) and integrity tests of the CM binaries.

9.1.1 Powerup Self-tests (Includes Known Answer Tests and Integrity Test)

Following powerup self-tests are performed by the module on power-up:

- AES-ECB 128 encrypt
- AES-ECB 128 decrypt
- HMAC-SHA2-256 Firmware Integrity Test
- SHA2-512

9.1.2 Conditional Tests

Following conditional tests are performed by the module:

- XTS Key Comparison Test

10 User Guidance

No specific user guidance is required for secure operation of the module. Any use of the non-Approved services as stated in Section 4.2 will result in a non-Approved mode of operation.

11 Crypto Officer Guidance

In order to install the FIPS validated module, the subsequent steps must be followed:

- AL5+ must be physically assembled on the PCB.
- Proper bootloader images must be programmed to SPI flash memory on PCB.
- User applications must be built by dynamically linking libalfips.so.
- AL5+ Carbon Linux, applications, libalfips.so and alfips.hmac must be installed. Installation shall be done by either programming images to SPI flash memory or downloading images from the network via tftp.
- Upon launching, the applications initialize the library which automatically performs the power-on self-test and integrity test. The libalfips.so and alfips.hmac file streams are loaded into the module and verified during its initialization call.
- The user applications shall be aborted and terminated if any power-on self-test (known-answer test or integrity test) fails.
- The user applications shall be aborted and terminated if the user applications request crypto operations without calling the module's initialization APIs. No operation can be performed until the module has completed its initialization (and passed its power-on self-tests).

The crypto officer is able to determine the status of the Approved mode by observing that the application initializes successfully. If any of the power on self-tests were to fail, the module would not be operational.

The calling application shall not request any non-Approved services while in the Approved mode. Doing so will result in a transition to a non-Approved state. All power-on self-tests are run before the module transitions to either an Approved or non-Approved state. CSPs are not shared between the Approved and non-Approved modes.