NetApp CryptoMod Version 2.1

FIPS 140-2 Non-Proprietary Security Policy

NetApp, Inc.
May 4th, 2020

Prepared by:

2400 Research Blvd, Suite 395
Rockville, MD 20850
tel: +1 (703) 375-9820
info@acumensecurity.net
www.acumensecurity.net

TABLE OF CONTENTS

1 Introduction 4

1.1 Purpose…….. 4

1.2 Document Organization 4

1.3 Notices…. 4

2 NetApp CryptoMod 5

2.1 Cryptographic Module Specification 5

2.1.1 Cryptographic Boundary 6

2.1.2 Modes of Operation 6

2.2 Cryptographic Module Ports and Interfaces 7

2.3 Roles, Services and Authentication 8

2.3.1 Roles……… 8

2.3.2 Authentication 8

2.3.3 Services…… 8

2.4 Physical Security 10

2.5 Operational Environment 10

2.6 Cryptographic Key Management 11

2.6.1 Key Generation 12

2.6.2 Key Storage... 12

2.6.3 Key Entry/Output 12

2.6.4 Zeroization Procedures 12

2.7 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) 13

2.8 Self-Tests…. 13

2.8.1 Power-On Self-Tests 13

2.8.2 Conditional Self-Tests 13

2.8.3 Self-Tests Error Handling 13

2.9 Mitigation of Other Attacks 14

3 Secure Operation 14

3.1 Installation… 14

3.2 Initialization.. 14

3.3 User Guidance 14

3.3.1 Usage of the Password-Based Key Derivation Function (PBKDF2) 14

3.3.2 Usage of the AES GCM 14

3.3.3 Usage of the AES-XTS mode 15

Appendix A: Acronyms 16

LIST OF TABLES

Table 1 - FIPS 140-2 Security Levels....5

Table 2 - Approved Algorithms....7

Table 3 - Ports and Interfaces....8

Table 4 - Approved Services....9

Table 5 - Non-Approved Services....10

Table 6 - Keys and CSPs....12

Table 7 - Acronyms....16

LIST OF FIGURES

Figure 1 - Block Diagram....6

1 Introduction

This is a non-proprietary FIPS 140-2 Security Policy for NetApp CryptoMod. Below are the details of the product certified:

Software Version #: 2.1

1.1 Purpose

This document was prepared as Federal Information Processing Standard (FIPS) 140-2 validation process. The document describes how CryptoMod meets the security requirements of FIPS 140-2. It also provides instructions to individuals and organizations on how to deploy the product in a secure FIPS-approved mode of operation. Target audience of this document is anyone who wishes to use or integrate this product into a solution that is meant to comply with FIPS 140-2 requirements.

1.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence Document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Acumen Security. under contract to NetApp, Inc.. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to NetApp, Inc and is releasable only under appropriate non-disclosure agreements.

1.3 Notices

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

2 NetApp CryptoMod

The NetApp CryptoMod, here-by referred to as CryptoMod or the module is a multi-chip standalone module validated at FIPS 140-2 Security Level 1. Specifically, the module meets that following security levels for individual sections in FIPS 140-2 standard:

#	Section Title	Security Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	1
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1
7	Cryptographic Key Management	1
8	EMI/EMC	1
9	Self-Tests	1
10	Design Assurances	1
11	Mitigation Of Other Attacks	N/A

Table 1 - FIPS 140-2 Security Levels

2.1 Cryptographic Module Specification

CryptoMod is a software cryptographic module whose purpose is to provide encryption/decryption for NetApp's ONTAP OS kernel. The CryptoMod module makes use of the AES-NI instruction set in Intel processors. Since CryptoMod can support non-PAA implementations as well as PAA implementations of the pertinent cryptographic algorithms, CryptoMod is designated as a software only cryptographic module.

2.1.1 Cryptographic Boundary

The logical cryptographic boundary of the CryptoMod module is the cryptomod_fips.ko component of ONTAP OS kernel. The logical boundary is depicted in the block diagram below. The Approved DRBG is used to supply the module's cryptographic keys. The physical boundary for the module is the enclosure of the NetApp controller.

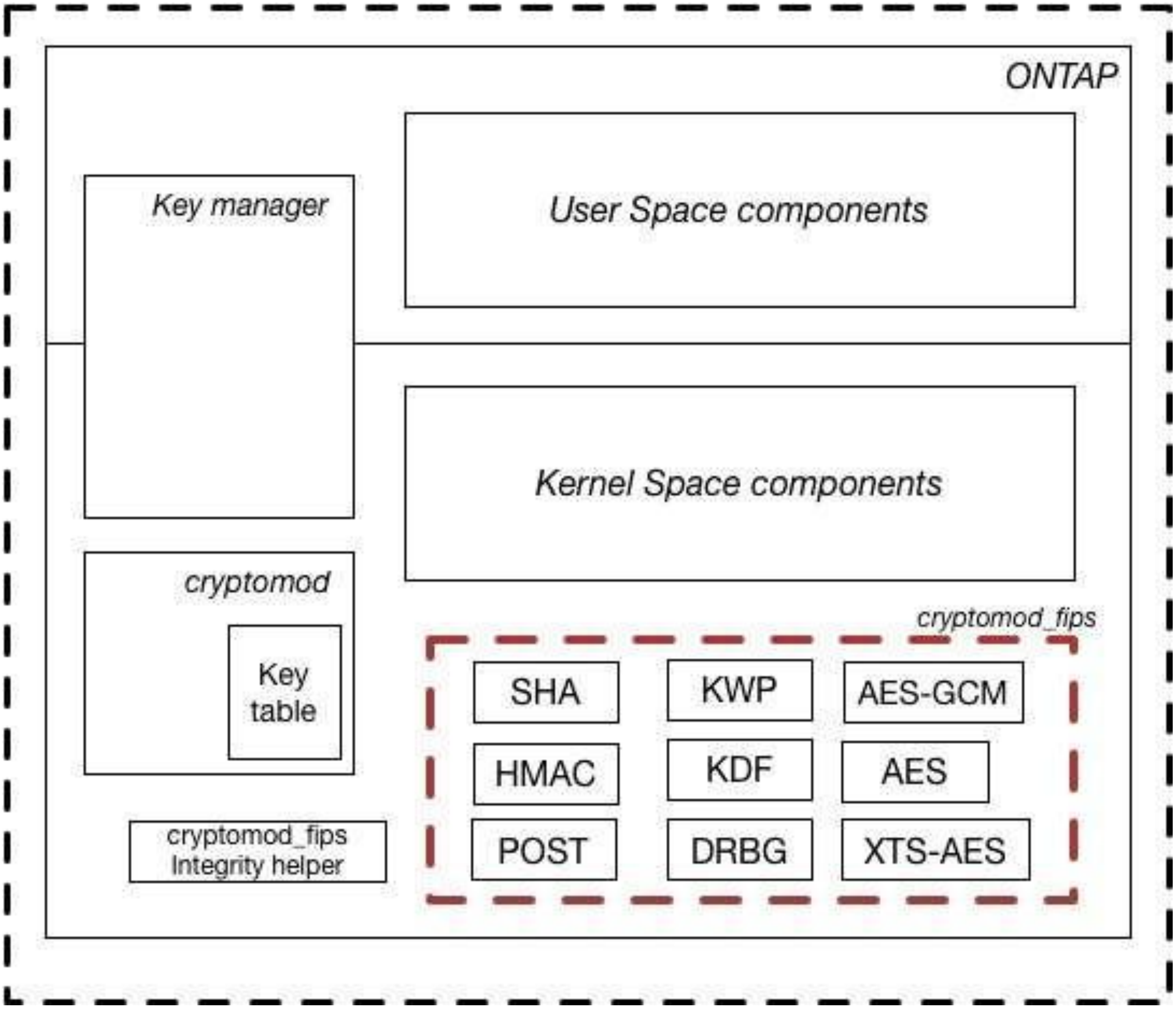

Figure 1 - Block Diagram

2.1.2 Modes of Operation

The module supports two modes of operation: Approved and Non-approved. The module will be in FIPS-approved mode when all power up self-tests have completed successfully and only Approved algorithms are invoked. See Table 2 below for a list of the supported Approved algorithms.

Cryptographic Algorithm	CAVP Cert #	Usage
AES (XTS, ECB, CBC, CTR, KWP)	5917	Symmetric encryption/decryption
AES GCM	5917	Authenticated encryption/Authenticated decryption
KTS	5917	Key Wrapping, Key Unwrapping
CKG	Vendor Affirmed	Cryptographic Key Generation
DRBG (CTR_DRBG)	2477	Random Bit Generation
SHA-1	4673	Message Digest
SHA-256	4673	Message Digest
SHA-512	4673	Message Digest
HMAC SHA-1	3897	Message Authentication
HMAC SHA-256	3897	Message Authentication, Key Establishment
HMAC SHA-512	3897	Message Authentication

Table 2 - Approved Algorithms

The module supports the following key agreement technique:

- KTS (AES Cert. #5917, key wrapping; key agreement methodology provides 256 bits of encryption strength);

The module supports the following non-FIPS 140-2 Approved but allowed algorithms that may be used in the Approved mode of operation:

- NDRNG (used to seed the Approved DRBG).

The module supports the following Vendor Affirmed security functions which are permitted for use in the FIPS approved mode:

- PBKDF2 (NIST SP 800-132) The vendor affirms compliance with SP 800-132, using option 1(a) in Section 5.4
- CKG (SP 800-133).

The module supports the following non-FIPS approved algorithms which are not permitted for use in the FIPS approved mode:

- SP 800-108 KBKDF (non-compliant)

2.2 Cryptographic Module Ports and Interfaces

As a software only module, CryptoMod does not have any physical ports. The physical ports are considered to be the ports on the device on which the module is running. The logical interfaces for the module are defined by the API for CryptoMod. If the module enters an error state then control and data output interfaces are disabled.

FIPS Interface	Physical Interface	Logical Interface
Data Input	Ethernet SATA/SAS/NVMe interfaces	Data passed to the API calls to be used by CryptoMod
Data Output	Ethernet SATA/SAS/NVMe interfaces	Data returned by API calls to CryptoMod
Control Input	Ethernet	Control data passed to the API calls to be used by CryptoMod
Control Output	Ethernet	Control data returned by API calls to CryptoMod
Status Output	Ethernet	Status data returned by API calls to CryptoMod

Table 3 - Ports and Interfaces

2.3 Roles, Services and Authentication

2.3.1 Roles

The module supports the following roles:

- User role: performs cryptographic functions and can check version information and status.
- Crypto-Officer role: can check version information and status, performs the module setup and configuration, module initialization, on-demand self-tests and zeroization.

The User and Crypto-Officer roles are implicitly assumed by the entity accessing the module services.

2.3.2 Authentication

The module is a Level 1 software-only cryptographic module and does not implement authentication. The roles are implicitly assumed based on the service requested.

2.3.3 Services

The module supports services available to users in the available roles. The following table shows the available services, the roles allowed, the Critical Security Parameters involved and how they are accessed in the Approved mode of operation.

Service	Description	Key/CSP	Role	Type of Access
Show version information	Returns the name of the module and the version associated with the module	N/A	User and Crypto-Officer	R, X
Show status	Returns the current status associated with the module	N/A	User and Crypto-Officer	R, X

Service	Description	Key/CSP	Role	Type of Access
Perform on demand self-tests	Initiates and runs the pre-operational self-tests specified.	N/A	Crypto-Officer	R, X
Encryption/Decryption	Perform encryption/decryption using AES.	128 and 256-bits AES keys Note: XTS mode only with 128 and 256 bit keys	User	R, W, X
Authenticated Encryption/Decryption	Perform authenticated encryption/decryption using AES GCM.	128 and 256-bits AES keys Note: GCM mode only with 128 and 256 bit keys	User	R, W, X
Key Wrapping/Key Unwrapping	Perform key wrapping/unwrapping using AES.	128 and 256-bits AES keys	User	R, W, X
Random Bit Generation	Provide random bits from the DRBG	Entropy input string, V values and Key	User	R, W, X
Key Generation	Perform Key Generation using the DRBG	128 and 256-bits AES keys	User	R, W, X
Message Authentication	Perform key-hash using HMAC	160 – 512-bits HMAC keys	User	R, W, X
Hashing	Perform SHA hashing function	N/A	User	N/A
Key Derivation Function	Perform Key Derivation using PBKDF2	256-bit AES key	User	R, W, X
Perform zeroization	Zeroize keys and critical security parameters stored in the Cryptomod key table	N/A	Crypto-Officer	R, X

Table 4 - Approved Services

R – Read, W – Write, X – Execute

The module also provides the following non-Approved services:

Service	Non-Approved Function(s)	Key/CSP	Role
Key Derivation Function	KDF in CTR Mode	N/A	User
AES GCM	Non-Conformant	N/A	User

Table 5 - Non-Approved Services

2.4 Physical Security

The module is comprised of software only and thus does not claim any physical security.

2.5 Operational Environment

The tested operating systems segregate user processes into separate process spaces. Each process space is logically separated from all other processes by the operating system software and hardware. The Module functions entirely within the process space of the calling application, and implicitly satisfies the FIPS 140-2 requirement for a single user mode of operation.

For FIPS 140-2 validation, the module is tested by an accredited FIPS 140-2 testing laboratory on the following operating environment:

- ONTAP 9.4 on a FAS2750 system with PAA; and

- ONTAP 9.4 on a FAS2750 system without PAA.

- ONTAP 9.4 on a AFF A800 system with PAA; and

- ONTAP 9.4 on a AFF A800 system without PAA.

Additionally, only when the module operates on the following platform, the module will remain compliant with FIPS 140-2 validation status because it is possible to operate without any source code change:

- ONTAP 9.4 on a FAS2620 (vendor affirmed);
- ONTAP 9.4 on a FAS2650 (vendor affirmed);
- ONTAP 9.4 on a FAS2720 (vendor affirmed);
- ONTAP 9.4 on a FAS8020 (vendor affirmed);
- ONTAP 9.4 on a FAS8040 (vendor affirmed);
- ONTAP 9.4 on a FAS8060 (vendor affirmed);
- ONTAP 9.4 on a FAS8080 EX (vendor affirmed);
- ONTAP 9.4 on a FAS8200 (vendor affirmed);
- ONTAP 9.4 on a FAS9000 (vendor affirmed);
- ONTAP 9.4 on a AFF8020 (vendor affirmed);
- ONTAP 9.4 on a AFF8040 (vendor affirmed);
- ONTAP 9.4 on a AFF8060 (vendor affirmed);
- ONTAP 9.4 on a AFF8080 EX (vendor affirmed);
- ONTAP 9.4 on a AFF A200 (vendor affirmed);
- ONTAP 9.4 on a AFF A220 (vendor affirmed);
- ONTAP 9.4 on a AFF A300 (vendor affirmed);
- ONTAP 9.4 on a AFF A700 (vendor affirmed);
- ONTAP 9.4 on a AFF A700s (vendor affirmed);
- ONTAP Select 9.4 on VMware ESXi 5.5 vSphere (vendor affirmed);
- ONTAP Select 9.4 on VMware ESXi 6.0 vSphere (vendor affirmed);
- ONTAP Select 9.4 on VMware ESXi 6.5 vSphere (vendor affirmed);

- ONTAP Select 9.4 on VMware ESXi 6.7 vSphere (vendor affirmed);
- ONTAP Select 9.4 on KVM version 1.5.3 on RedHat Enterprise Linux 7.4 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 1.5.3 on RedHat Enterprise Linux 7.5 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 2.9.0 on RedHat Enterprise Linux 7.4 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 2.9.0 on RedHat Enterprise Linux 7.5 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 1.5.3 on Oracle Linux 7.4 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 1.5.3 on Oracle Linux 7.5 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 2.9.0 on Oracle Linux 7.4 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 2.9.0 on Oracle Linux 7.5 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 1.5.3 on CentOS 7.4 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 1.5.3 on CentOS 7.5 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 2.9.0 on CentOS 7.4 (vendor affirmed);
- ONTAP Select 9.4 on KVM version 2.9.0 on CentOS 7.5 (vendor affirmed);
- ONTAP Cloud Volumes 9.4 running on AWS (vendor affirmed); and
- ONTAP Cloud Volumes 9.4 running on Azure (vendor affirmed).

As per FIPS 140-2 Implementation Guidance G.5, compliance is maintained for other versions of the respective operational environments where the module binary is unchanged. No claim can be made as to the correct operation of the module or the security strengths of the generated keys if any source code is changed and the module binary is reconstructed.

The GPC(s) used during testing met Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part 15, Subpart B. FIPS 140-2 validation compliance is maintained when the module is operated on other versions of the GPOS running in single user mode, assuming that the requirements outlined in NIST IG G.5 are met.

The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

2.6 Cryptographic Key Management

The module supports the following keys and critical security parameters (CSPs):

Key/CSP Name	Key Description	Generation/Input	Output
DRBG V Value	128-bits	Internally generated	Does not exit the module
DRBG Internal State Key	256-bits	Internally generated	Does not exit the module
DRBG Entropy Input String	384-bits	Input via API in plaintext	Does not exit the module
DRBG Seed	384-bits	Input from entropy source	Does not exit the module

Key/CSP Name	Key Description	Generation/Input	Output
AES Encrypt/Decrypt Key	AES (128 and 256-bits) encrypt / decrypt key	Generated internally using the Approved DRBG or input via API in plaintext	Output via API in plaintext
AES Wrapping/Uwrapping Key	AES (128 and 256-bits) key wrapping key	Generated internally using the Approved DRBG or input via API in plaintext	Output via API in plaintext
AES GCM Key	AES GCM (128 and 256-bits) encrypt / decrypt key	Generated internally using the Approved DRBG or input via API in plaintext	Output via API in plaintext
AES XTS Key	AES XTS (128 and 256-bits) encrypt / decrypt key	Generated internally using the Approved DRBG or input via API in plaintext	Output via API in plaintext
HMAC Key	Keyed-hash key (160/224/256/384 and 512-bits)	Input via API in plaintext	Output via API in plaintext
CPKEK key	AES (256-bits)	Derived via PBKDF2 from a passphrase input via API in plaintext	Output via API in plaintext

Table 6 - Keys and CSPs

2.6.1 Key Generation

CryptoMod implements a NIST SP 800-90A DRBG for the generation of random bits and keys. The implementation of CTR_DRBG uses AES-256 (maximum of 256 bits of security strength) as the block cipher along with the appropriate derivation function.

On the tested system entropy is provided from the Operating System’s /dev/random in addition to Intel’s RDRAND instruction set. The module requests a minimum number of 384 bits of entropy from its Operational Environment per each call.

2.6.2 Key Storage

The cryptographic module does not perform persistent storage of keys. Keys and CSPs are passed to the module by the calling kernel process. The keys and CSPs are stored in memory in plaintext. Keys and CSPs residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the module defined API. The ONTAP operating system protects memory and process space from unauthorized access.

2.6.3 Key Entry/Output

Symmetric keys are provided to the module by the calling process, and are destroyed when released by the appropriate API function calls. The module does not perform persistent storage of keys.

2.6.4 Zeroization Procedures

Keys can be zeroized by an application requesting that CryptoMod zero the key associated with a given key ID, or by rebooting the host NetApp controller. Prior to being zeroed, the key contents are overwritten with random data.

2.7 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The NetApp controllers (FAS2750 and AFF A800 systems) have been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules.

2.8 Self-Tests

Self-tests are health checks that ensure the cryptographic algorithms implemented within the module are operating correctly. The self-tests identified in FIPS 140-2 broadly fall within two categories:

1. Power-On Self-Tests
2. Conditional Self-Tests

The Crypto-Officer with physical or logical access to the module can run the POST (Power-On Self-Tests) on demand by power cycling the module or by rebooting the operating system.

2.8.1 Power-On Self-Tests

The CryptoMod module performs the following self-tests at startup:

1. Known Answer Test: KATs are performed for the following algorithms.
    - AES encrypt and decrypt
    - AES GCM encrypt and decrypt
    - DRBG
    - HMAC SHA-1
    - HMAC SHA-256
    - HMAC SHA-512
    - PBKDF2
    - SHA-1
    - SHA-256
    - SHA-512
    - XTS-AES encrypt and decrypt
2. Software Integrity Test: The stored HMAC-SHA-256 values are checked by the module at power-up.

2.8.2 Conditional Self-Tests

The module performs the following conditional self-tests:

- NIST SP 800-90Arev1 Section 11 DRBG Health Tests; and
- CRNGT on the NDRNG.

2.8.3 Self-Tests Error Handling

If any of the power-up self-tests fail, the module enters an error state and ceases operation, inhibiting any further data output. The module does not perform any cryptographic operations while in an error state.

If the module enters an error state, the Crypto-Officer must reboot the system to perform power-up self-tests. Successful completion of the power-up self-tests will return the module to normal operation.

2.9 Mitigation of Other Attacks

This section is not applicable. The module does not claim to mitigate any attacks beyond the FIPS 140-2 requirements for a level 1 module.

3 Secure Operation

3.1 Installation

The module consists of a single kernel object module that provides cryptographic services as part of the NetApp ONTAP operating system. The sections below describe how to install, configure, and keep the module in a FIPS-approved mode of operation.

3.2 Initialization

The module is initialized during the operating system boot sequence, before any cryptographic functionality is available.

3.3 User Guidance

There is no FIPS 140-2 specific guidance required to place the module into its Approved mode of operation.

3.3.1 Usage of the Password-Based Key Derivation Function (PBKDF2)

In line with the requirements for SP 800-132, keys generated using the approved PBKDF2 must only be used for storage applications. Any other use of the approved PBKDF2 is noncompliant.

As the module is a general purpose software module, it is not possible to predict the use of the PBKDF2, however a user of the module should also note that a password should at least contain enough entropy to be unguessable and also contain enough entropy to reflect the security strength required for the key being generated. Users are referred to Appendix A, “Security Considerations” of SP 800-132 for further information on password, salt, and iteration count selection.

3.3.2 Usage of the AES GCM

AES GCM encryption and decryption is primarily used in the context of ONTAP kernel channels encrypted with TLS protocol version 1.2 and clients connecting to ONTAP via SMB 3.0.

The module's AES-GCM implementation conforms to IG A.5, scenario #1, following RFC 5288 for TLS 1.2. The counter portion of the IV is set by the module within its cryptographic boundary. The module ensures that it's strictly increasing and thus cannot repeat. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key in accordance with RFC 5246.

The IV generation method is user selectable and the value can be computed in more than one manner. The selection of the IV construction method is the responsibility of the user of this cryptographic module. In approved mode, users of the module must not utilize GCM with an externally generated IV.

In case the module's power is lost and then restored, the key used for AES GCM encryption or decryption shall be re-distributed.

3.3.3 Usage of the AES-XTS mode

Per the requirements of SP 800-38E, AES-XTS mode shall be used for storage purposes only.

Appendix A: Acronyms

This section describes the acronyms used throughout the document.

Acronym	Definition
AES	Advanced Encryption Standard
AES-NI	Advanced Encryption Standard New Instructions
API	Application Program Interface
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CMVP	Crypto Module Validation Program
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CTR	Counter
DRBG	Detrministic Random Bit Generator
ECB	Electronic Codebook
FIPS	Federal Information Processing
GCM	Galois Counter Mode
GPC	General Purpose Computer
HMAC	Hashed Message Authentication
KAT	Known Answer Test
KDF	Key Derivation Function
KTS	Key Transport Scheme
KWP	Key Wrap with Padding
NDRNG	Non-Deterministic Random Number Generator
NVMe	Non-Volatile Memory Express
OS	Operating System
PAA	Processor Assisted Acceleration
PBKDF2	Password-Based Key Derivation Function, Version 2
POST	Power On Self-Test
SAS	Serial Attached SCSI
SATA	Serial ATA
SHA	Secure Hash Algorithm
XTS	XOR-Encrypt-XOR-Based Tweaked Code Book wth Ciphertext Stealing

Table 7 - Acronyms