NetApp CryptoMod Version 2.2

FIPS 140-2 Non-Proprietary Security Policy

NetApp, Inc.

September 10, 2021

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 ... 7
2.2 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES ... 8
2.3 ROLES, SERVICES AND AUTHENTICATION ... 9
2.3.1 ROLES ... 9
2.3.2 AUTHENTICATION ... 9
2.3.3 SERVICES ... 9
2.4 PHYSICAL SECURITY ... 10
2.5 OPERATIONAL ENVIRONMENT ... 10
2.6 CRYPTOGRAPHIC KEY MANAGEMENT ... 13
2.6.1 KEY GENERATION ... 13
2.6.2 KEY STORAGE ... 14
2.6.3 KEY ENTRY/OUTPUT ... 14
2.6.4 ZEROIZATION PROCEDURES ... 14
2.7 ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY (EMI/EMC) ... 14
2.8 SELF-TESTS ... 14
2.8.1 POWER-ON SELF-TESTS ... 14
2.8.2 CONDITIONAL SELF-TESTS ... 15
2.8.3 SELF-TESTS ERROR HANDLING ... 15
2.9 MITIGATION OF OTHER ATTACKS ... 15

3 SECURE OPERATION ... 15

3.1 INSTALLATION ... 15
3.2 INITIALIZATION ... 15
3.3 USER GUIDANCE ... 15
3.3.1 USAGE OF THE PASSWORD-BASED KEY DERIVATION FUNCTION (PBKDF2) ... 16
3.3.2 USAGE OF THE AES GCM ... 16
3.3.3 USAGE OF THE AES-XTS MODE ... 16

APPENDIX A: ACRONYMS ... 17

APPENDIX B: REFERENCES ... 18

LIST OF TABLES

Table 1: FIPS 140-2 Security Levels ... 5
Table 2: Approved Algorithms ... 7
Table 3: Allowed Algorithms ... 8
Table 4: Ports and Interfaces ... 8
Table 5: User and Crypto-Officer Services ... 9
Table 6: Keys and Critical Security Parameters ... 13

Table 7: Acronyms... 17

LIST OF FIGURES

Figure 1: Block Diagram 6

1 Introduction

This is a non-proprietary FIPS 140-2 Security Policy for NetApp CryptoMod version 2.2. Below are the details of the product certified:

Software Version #: 2.2

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

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 the following security levels for individual sections in FIPS 140-2 standard:

Table 1: FIPS 140-2 Security Levels

#	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

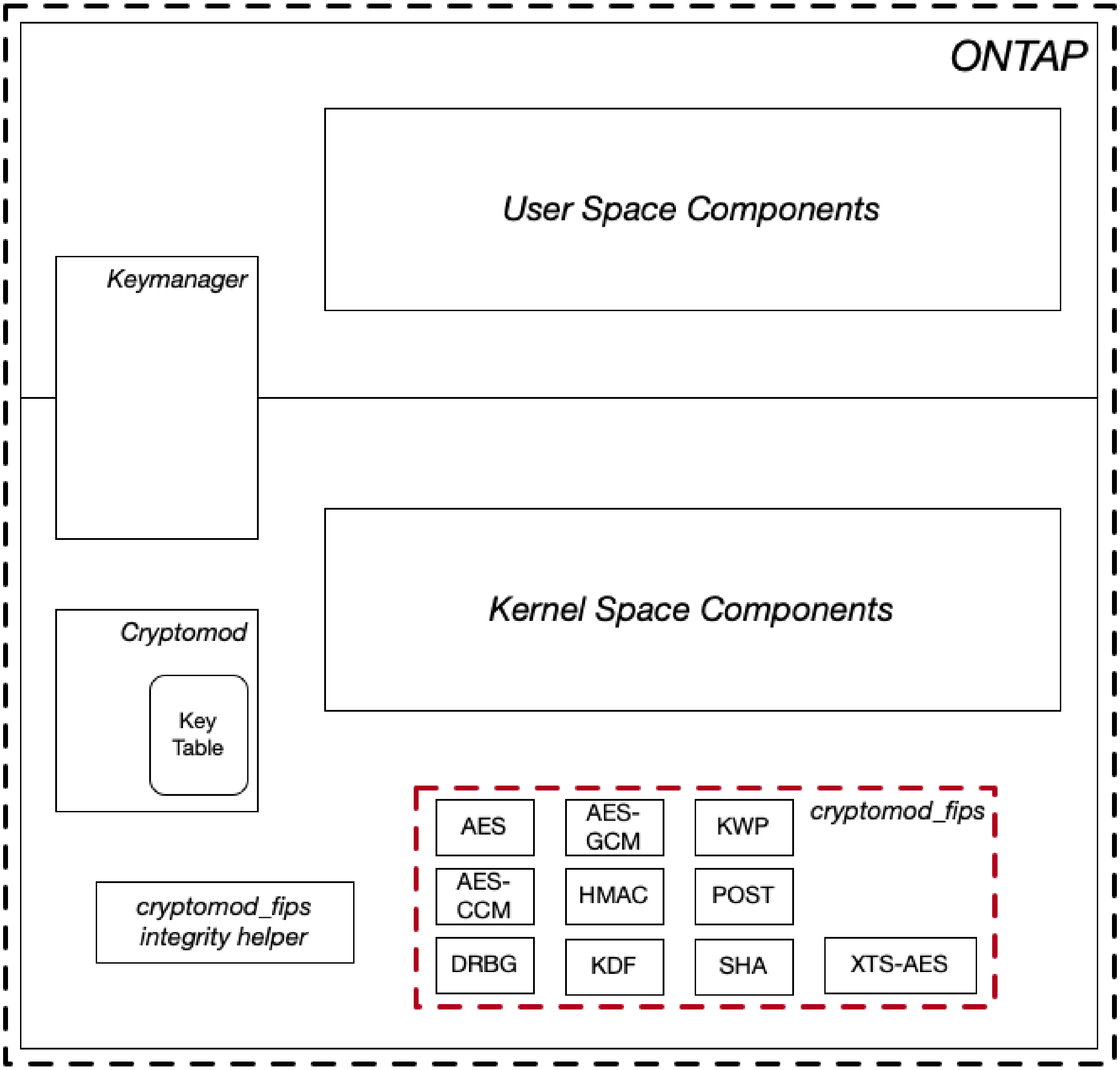
2.1 Cryptographic Module Specification

CryptoMod is a software cryptographic module whose purpose is to provide encryption/decryption for NetApp's ONTAP Operating System (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 one mode of operation: Approved. The module will be in the FIPS- approved mode when all power up self-tests have completed successfully, and only Approved algorithms are invoked. If the power up self-tests fail, then the module reboots the NetApp controller. See Table 2 below for a list of the supported Approved algorithms.

Table 2: Approved Algorithms

Algorithm	Mode/Method	Key Lengths (bits)	Use	Standard	CAVP Certs
AES	CBC	128, 256	Data encryption and decryption	[FIPS-197] [SP800-38A]	PAA mode: #C1884 Non-PAA mode: #C1885
	CCM	128	Data encryption and decryption	[SP800-38C]	PAA mode: #C1884 Non-PAA mode: #C1885
	ECB	128, 256	Data encryption and decryption	[FIPS-197] [SP800-38A]	PAA mode: #C1884 Non-PAA mode: #C1885
	GCM	128, 256	Data encryption and decryption	[SP800-38D]	PAA mode: #C1884 Non-PAA mode: #C1885
	GMAC	128, 256	MAC generation and verification	[SP800-38D]	PAA mode: #C1884 Non-PAA mode: #C1885
	KWP	256	Key wrapping and unwrapping	[SP800-38F]	PAA mode: #C1884 Non-PAA mode: #C1885
	XTS	128, 256	Data encryption and decryption for data storage	[SP800-38E]	PAA mode: #C1884 Non-PAA mode: #C1885
KTS	AES KWP	256	Key wrapping and unwrapping	[SP800-38F]	PAA mode: #C1884 Non-PAA mode: #C1885
CKG	KDF in CTR mode [SP800-108]	256	Symmetric key generation	[SP800-133]	Vendor affirmed compliance to [SP800-133] section 6.2.2 from a KDF and a different preexisting key as specified in

Algorithm	Mode/Method	Key Lengths (bits)	Use	Standard	CAVP Certs
					[SP800-108]
DRBG	CTR_DRBG: AES-256 with derivation function and prediction resistance	N/A	Deterministic random bit generation	[SP800-90A]	PAA mode: #C1884 Non-PAA mode: #C1885
HMAC	HMAC SHA-1 HMAC SHA-256 HMAC SHA-512		Message authentication code	[FIPS 198-1]	PAA mode: #C1884 Non-PAA mode: #C1885
PBKDF2	HMAC SHA-1 HMAC SHA-256 HMAC SHA-512		Symmetric key generation	[SP800-132]	Vendor affirmed compliance with [SP800-132] using option 1(a) in section 5.4
SHS	SHA-1 SHA-256 SHA-512	N/A	Message digest	[FIPS 180-4]	PAA mode: #C1884 Non-PAA mode: #C1885

The module supports the following key establishment method:

- KTS (AES Certs. #C1884 and #C1885);

Table 3 contains a list of non-FIPS 140-2 Approved but allowed algorithms that may be used in the Approved mode of operation.

Table 3: Allowed Algorithms

Cryptographic Algorithm	Usage
NDRNG	Used to seed the approved DRBG

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. Table 4, below, lists the ports and interfaces associated with the module.

Table 4: Ports and Interfaces

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

FIPS Interface	Physical Interface	Logical Interface
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

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 (CSP) involved and how they are accessed in the Approved mode of operation.

In the table below, R – Read, W – Write, X – Execute.

Table 5: User and Crypto-Officer Services

Service	Description	Key/CSP	Role	Type of Access	Inputs	Outputs
Show version information	Returns the name of the module and the version associated with the module	N/A	User and Crypto-Officer	R, X	Command and parameters	Command response/Return code
Show status	Returns the current status associated with the module	N/A	User and Crypto-Officer	R, X	Command and parameters	Command response/Return code
Perform on demand self-tests	Initiates and runs the pre-operational self-tests specified.	N/A	Crypto-Officer	R, X	Reboot	Command response/Return code

Service	Description	Key/CSP	Role	Type of Access	Inputs	Outputs
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	Command and parameters	Command response/Return code
Authenticated Encryption/Decryption	Perform authenticated encryption/decryption using AES GCM and AES CCM.	128 and 256-bits AES keys. Note 1: GCM mode only with 128- and 256-bit keys. Note 2: CCM PAA mode: 128-bit keys only. CCM non-PAA mode: 128- and 256-bit keys.	User	R, W, X	Command and parameters	Command response/Return code
Key Wrapping/Key Unwrapping	Perform key wrapping/unwrapping using AES.	128 and 256-bits AES keys	User	R, W, X	Command and parameters	Command response/Return code
Random Bit Generation	Provide random bits from the DRBG	Entropy input string, V values and Key	User	R, W, X	Command and parameters	Command response/Return code
Key Generation	Perform Key Generation using the DRBG	128 and 256-bits AES keys	User	R, W, X	Command and parameters	Command response/Return code
Message Authentication	Perform key hash using HMAC	160 – 512-bits HMAC keys	User	R, W, X	Command and parameters	Command response/Return code
Hashing	Perform SHA hashing function	N/A	User	N/A	Command and parameters	Command response/Return code
Key Derivation Function	Perform Key Derivation using PBKDF2	256-bit AES key	User	R, W, X	Command and parameters	Command response/Return code
Key Derivation Function	Perform Key Derivation using NIST SP800-108 KDF in CTR mode	256-bit AES key	User	R, W, X	Command and parameters	Command response/Return code
Zeroize	Zeroize keys and CSPs	All	User and Crypto-Officer	W	Reboot	N/A

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 environments:

- ONTAP 9.7P6 running on AFF A800 system with an Intel® Xeon® Platinum 8160 with PAA;
- ONTAP 9.7P6 running on AFF A800 system with an Intel® Xeon® Platinum 8160 without PAA;
- ONTAP 9.7P6 running on FAS2650 system with an Intel® Xeon® D-1528 with PAA;
- ONTAP 9.7P6 running on FAS2650 system with an Intel® Xeon® D-1528 without PAA;
- ONTAP 9.7P6 running on FAS8300 system with an Intel® Xeon® Silver 4210 with PAA; and
- ONTAP 9.7P6 running on FAS8300 system with an Intel® Xeon® Silver 4210 without PAA;

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

- FAS models:
  - ONTAP 9.7P6 running on FAS 2620 (vendor affirmed);
  - ONTAP 9.7P6 running on FAS 2720 (vendor affirmed);
  - ONTAP 9.7P6 running on FAS 2750 (vendor affirmed);
  - ONTAP 9.7P6 running on FAS 8020 (vendor affirmed)
  - ONTAP 9.7P6 running on FAS 8040 (vendor affirmed);
  - ONTAP 9.7P6 running on FAS 8060 (vendor affirmed);
  - ONTAP 9.7P6 running on FAS 8080 EX (vendor affirmed);
  - ONTAP 9.7P6 running on FAS 8200 (vendor affirmed);
  - ONTAP 9.7P6 running on FAS 8700 (vendor affirmed); and
  - ONTAP 9.7P6 running on FAS 9000 (vendor affirmed);
- AFF models:
  - ONTAP 9.7P6 running on AFF 8020 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF 8040 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF 8060 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF 8080 EX (vendor affirmed);
  - ONTAP 9.7P6 running on AFF A200 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF A220 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF A300 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF A320 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF A400 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF A700 (vendor affirmed);
  - ONTAP 9.7P6 running on AFF A700s (vendor affirmed); and
  - ONTAP 9.7P6 running on AFF C190 (vendor affirmed).
- ASA (All SAN Array) AFF models:
  - ONTAP 9.7P6 running on ASA A220 (vendor affirmed);
  - ONTAP 9.7P6 running on ASA A400 (vendor affirmed); and
  - ONTAP 9.7P6 running on ASA A700 (vendor affirmed).
- ONTAP Select models:

    - ONTAP Select 9.7P6 running on VMware ESXi 6.0 vSphere (vendor affirmed);
    - ONTAP Select 9.7P6 running on VMware ESXi 6.5 vSphere (vendor affirmed);
    - ONTAP Select 9.7P6 running on VMware ESXi 6.7 vSphere (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 1.5.3 on RedHat Enterprise Linux 7.4 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 1.5.3 on RedHat Enterprise Linux 7.5 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 2.9.0 on RedHat Enterprise Linux 7.4 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 2.9.0 on RedHat Enterprise Linux 7.5 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 1.5.3 on Oracle Linux 7.4 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 1.5.3 on Oracle Linux 7.5 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 2.9.0 on Oracle Linux 7.4 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 2.9.0 on Oracle Linux 7.5 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 1.5.3 on CentOS 7.4 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 1.5.3 on CentOS 7.5 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 2.9.0 on CentOS 7.4 (vendor affirmed);
    - ONTAP Select 9.7P6 running on KVM version 2.9.0 on CentOS 7.5 (vendor affirmed);
- Cloud Volumes ONTAP models
    - Cloud Volumes ONTAP 9.7P6 running on Amazon Web Services (vendor affirmed); and
    - Cloud Volumes ONTAP 9.7P6 running on Microsoft 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):

Table 6: Keys and Critical Security Parameters

Key/CSP Name	Key Description	Generation/Input	Output	Zeroization
DRBG V Value	128-bits	Internally generated	Does not exit the module	Cleared on reboot
DRBG Internal State Key	256-bits	Internally generated	Does not exit the module	Cleared on reboot
DRBG Entropy Input String	384-bits	Input via API in plaintext	Does not exit the module	Cleared on reboot
DRBG Seed	384-bits	Input from entropy source	Does not exit the module	Cleared on reboot
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	Cleared on reboot
AES Wrapping/Unwrapping 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	Cleared on reboot
AES CCM Key	AES CCM (128 and 256-bits) encrypt / decrypt key	Generated internally using the Approved DRBG or input via API in plaintext	Output via API in plaintext	Cleared on reboot
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	Cleared on reboot
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	Cleared on reboot
HMAC Key	Keyed-hash key (160/224/256/384 and 512-bits)	Input via API in plaintext	Output via API in plaintext	Cleared on reboot
CPKEK Key	AES (256-bits)	Derived via PBKDF2 from a passphrase input via API in plaintext	Output via API in plaintext	Cleared on reboot
KDK Key	AES (256-bits)	Input via API in plaintext	Does not exit the module	Cleared on reboot
KDK Output Key	AES (256-bits)	Derived via KDF from the KDK key input via API in plaintext	Output via API in plaintext	Cleared on reboot

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 file 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.

In addition, the vendor affirmed CKG implementation uses an Approved counter DRBG specified in NIST SP 800-90Arev1. The key generation method adheres to NIST SP 800-133 and the module utilizes post processing. The output of the CryptoMod DRBG is XOR’d with a fixed mask to compute the secret value "K" as per example #1 in FIPS 140-2 IG 7.8. The postprocessing is performed on DRBG output and post-processing operation becomes the new "U".

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 non-dumpable 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 (overwritten with “zeroes”) by rebooting the host NetApp controller.

2.7 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The NetApp controllers (FAS and AFF 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 EBC encrypt and decrypt for 128 and 256-bit keys
    - AES GCM encrypt and decrypt for 128 and 256-bit keys
    - AES CCM encrypt and decrypt for a 128-bit key
    - DRBG
    - HMAC SHA-1
    - HMAC SHA-256
    - HMAC SHA-512

- SP800-108 KDF CTR mode
- PBKDF2
- SHA-1
- SHA-256
- SHA-512
- XTS-AES encrypt and decrypt for XTS-AES-128 and XTS-AES-256

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 800-90A Rev1 Section 11 DRBG Health Tests; and
- CRNGT on the NDRNG.

Per [SP800-90A], DRBG conditional self-tests are performed during the power-on self-testing sequence. The NDRNG continuous test (CRNGT) is performed whenever a random value is requested from the NDRNG.

2.8.3 Self-Tests Error Handling

If any of the power-up self-tests or conditional 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 contain at least enough entropyto 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

The AES GCM key and IV are passed to the module via an API call. It is the responsibility of the calling application to enforce A.5 requirements.

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.

Table 7: Acronyms

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	Deterministic 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 with Ciphertext Stealing

Appendix B: References

[FIPS 180-4] Secure Hash Standard (SHS)
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[FIPS 197] Advanced Encryption Standard
https://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[FIPS 198-1] The Keyed Hash Message Authentication Code (HMAC)
https://csrc.nist.gov/csrc/media/publications/fips/198/1/final/documents/fips-198-1_final.pdf

[SP 800-38A] NIST Special Publication 800-38A – Recommendation for Block Cipher Modes of Operation: Methods and Techniques
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[SP 800-38C] NIST Special Publication 800-38C – Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

[SP 800-38D] NIST Special Publication 800-38D – Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

[SP 800-38E] NIST Special Publication 800-38E – Recommendation for Block Cipher Modes of Operation: The XTS AES Mode for Confidentiality on Storage Devices
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38e.pdf

[SP 800-38F] NIST Special Publication 800-38F – Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38F.pdf

[SP 800-90A] NIST Special Publication 800-9A Revision 1 – Recommendation for Random Number Generation Using Deterministic Random Bit Generators
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf

[SP 800-108] NIST Special Publication 800-108 (Revised) – Recommendation for Key Derivation Using Pseudorandom Functions
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf

[SP 800-133] NIST Special Publication 800-133 Revision 2 – Recommendation for Cryptographic Key Generation
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf