NetApp CryptoMod

3.0

FIPS 140-3 Non-Proprietary Security Policy

NetApp, Inc.
July 19, 2024

Document version: 0.10

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 General

The NetApp CryptoMod module, hereby referred to as either CryptoMod, or “the module”, is a multi-chip standalone module validated at FIPS 140-3 Security Level 1. Specifically, the module meets the following security levels for each of the individual sections in the FIPS 140-3 standard:

Table 1) Security Levels

ISO/IEC 24759 Section 6. [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic module specification	1
3	Cryptographic module interfaces	1
4	Roles, services, and authentication	1
5	Software/Firmware security	1
6	Operational environment	1
7	Physical security	N/A
8	Non-invasive security	1
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A

1.1 Introduction

This is the non-proprietary FIPS 140-3 Security Policy for NetApp CryptoMod version 3.0. Below are the details for the product being certified:

Software Version #: 3.0

1.2 Purpose

This document was prepared as part of a Federal Information Processing Standard (FIPS) 140-3 validation process. The document describes how CryptoMod meets the security requirements of FIPS 140-3. It also provides instructions to individuals and organizations on how to deploy the product in the approved mode of operation. The target audience for this document is anyone who wishes to use or integrate this product into a solution that is meant to comply with FIPS 140-3 requirements.

1.3 Document Organization

The Security Policy is one document in a FIPS 140-3 Submission Package. In addition to this document, the Submission Package contains:

- a Vendor Evidence document
- a Finite State Model description
- other supporting documentation as additional references.

Except for this non-proprietary Security Policy, the FIPS 140-3 Submission Package is proprietary to NetApp, Inc. and is releasable only under appropriate non-disclosure agreements.

1.4 Notices

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

2 Cryptographic module specification

CryptoMod is a software cryptographic module whose purpose is to provide encryption/decryption services 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.

For FIPS 140-3 validation, the module is tested by an accredited FIPS 140-3 testing laboratory on the following operating environments:

Table 2) Tested Operational Environments

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	ONTAP 9.11.1	AFF A250	Intel Xeon® D-2164IT	Yes/No
2	ONTAP 9.11.1	AFF A400	Intel Xeon Silver 4210	Yes/No
3	ONTAP 9.11.1	AFF A900	Intel Xeon Platinum 8352Y	Yes/No

Additionally, the vendor is affirming module compliance on the following platforms without any source code changes. See Table 3) Vendor Affirmed Operational Environments below.

Note: The CMVP makes no statement as to the correct operation of the module on the operational environments for which operational testing was not performed.

Table 3) Vendor Affirmed Operational Environments

#	Operating Systems	Hardware Platform
1	ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A150
2	ONTAP 9.15.0, ONTAP 9.15.1	AFF A1K
3	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A220
4	ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A250
5	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A300
6	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A320

#	Operating Systems	Hardware Platform
7	ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A400
8	ONTAP 9.15.0, ONTAP 9.15.1	AFF A70
9	ONTAP 9.15.0, ONTAP 9.15.1	AFF A90
10	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A700
11	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A700s
12	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A800
13	ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF A900
14	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF C190
15	ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF C250
16	ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF C400
17	ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AFF C800
18	ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA A150
19	ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA A250
20	ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA A400
21	ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA A800
22	ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA A900
23	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA AFF A220
24	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1	ASA AFF A250
25	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1	ASA AFF A400
26	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA AFF A700

#	Operating Systems	Hardware Platform
27	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1	ASA AFF A800
28	ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA C250
29	ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA C400
30	ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	ASA C800
31	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS2720
32	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS2750
33	ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS2820
34	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS500f
35	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS8200
36	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS8300
37	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS8700
38	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS9000
39	ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	FAS9500
40	Data ONTAP Select 9.11.1, Data ONTAP Select 9.12.1, Data ONTAP Select 9.13.1, Data ONTAP Select 9.14.1, Data ONTAP Select with VMware ESXi 7/8	FDvM300-16GB
41	Data ONTAP Select 9.11.1, Data ONTAP Select 9.12.1, Data ONTAP Select 9.13.1, Data ONTAP Select 9.14.1, Data ONTAP Select with VMware ESXi 7/8	FDvM300-64GB
42	Data ONTAP Select 9.11.1, Data ONTAP Select 9.12.1, Data ONTAP Select 9.13.1, Data ONTAP Select 9.14.1, Data ONTAP Select with VMware ESXi 7/8	FDvM300-128GB

#	Operating Systems	Hardware Platform
43	Amazon FSx for NetApp ONTAP 9.11.1, ONTAP 9.12.0, ONTAP 9.12.1, ONTAP 9.13.0, ONTAP 9.13.1, ONTAP 9.14.0, ONTAP 9.14.1, ONTAP 9.15.0, ONTAP 9.15.1	AWS EC2 Nitro[1]
44	Cloud Volumes ONTAP 9.11.1, Cloud Volumes ONTAP 9.12.0, Cloud Volumes ONTAP 9.12.1, Cloud Volumes ONTAP 9.13.0, Cloud Volumes ONTAP 9.13.1, Cloud Volumes ONTAP 9.14.0, Cloud Volumes ONTAP 9.14.1, Cloud Volumes ONTAP 9.15.0, Cloud Volumes ONTAP 9.15.1	Microsoft Azure Compute[2]
45	Cloud Volumes ONTAP 9.11.1, Cloud Volumes ONTAP 9.12.0, Cloud Volumes ONTAP 9.12.1, Cloud Volumes ONTAP 9.13.0, Cloud Volumes ONTAP 9.13.1, Cloud Volumes ONTAP 9.14.0, Cloud Volumes ONTAP 9.14.1, Cloud Volumes ONTAP 9.15.0, Cloud Volumes ONTAP 9.15.1	Google Compute Engine[3]

Modes of operation

The module supports one mode of operation: Approved. The module will be in the approved mode when all the 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 hardware platform. See Table 4) Approved Algorithms (below) for a list of the supported Approved algorithms.

Table 4) Approved Algorithms

CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s)/Key Strength(s)	Use/Function
A2640	AES [FIPS 197] [SP800-38A]	CBC	128, 256	Data encryption and decryption
A2640	AES [FIPS 197] [SP800-38C]	CCM	128	Data encryption and decryption
A2640	AES [FIPS 197] [SP800-38B]	CMAC	128, 256	Message authentication code
A2640	AES [FIPS-197] [SP800-38A]	ECB	128, 256	Data encryption and decryption

[1] See https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-aws.html
[2] See https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-azure.html
[3] See https://docs.netapp.com/us-en/cloud-volumes-ontap-relnotes/reference-configs-gcp.html

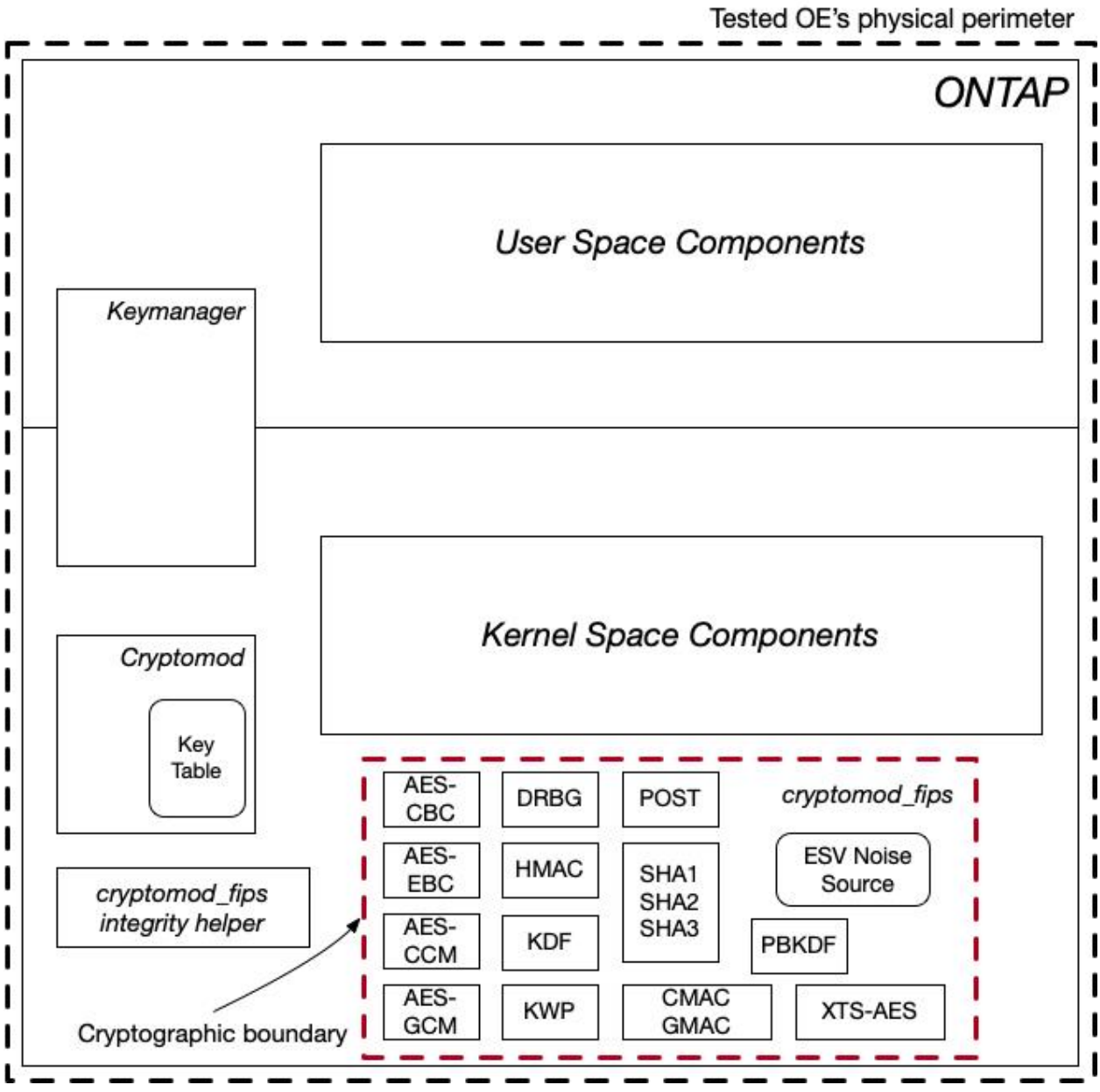
CAVP Cert	Algorithm and Standard	Mode/Method	Description/Key Size(s)/Key Strength(s)	Use/Function
A2640	AES [FIPS-197] [SP800-38D]	GCM	128, 256	Data encryption and decryption
A2640	AES [FIPS-197] [SP800-38D]	GMAC	128, 256	Message authentication code
A2640	AES [FIPS-197] [SP800-38F]	KWP	128, 256	Key wrapping and unwrapping
A2640	AES [FIPS-197] [SP800-38E]	XTS	128, 256	Data encryption and decryption for data storage
A2640	KTS [FIPS-197] [SP800-38F]	AES KWP	128, 256	Key wrapping and unwrapping
Vendor Affirmed	CKG [SP800-133rev2 Section 6.3 method 2]	XOR one symmetric key and one item of data	128,256	Symmetric key generation
A2640	KBKDF [SP800-108]	KBKDF in CTR mode	256	Symmetric key generation
A2640	DRBG [SP800-90Arev1]	CTR_DRBG: AES-256 with derivation function and predictive resistance	N/A	Deterministic random bit generation
A2640	HMAC [FIPS 198-1]	HMAC SHA-1 HMAC SHA2-256 HMAC SHA2-512	N/A	Keyed message authentication code
A2640	PBKDF [SP800-132]	HMAC SHA-1 HMAC SHA2-256 HMAC SHA2-512	112–4096	Symmetric key derivation
A2640	SHA-3 [FIPS 202]	SHA3-256	N/A	Message digest
A2640	SHS [FIPS 180-4]	SHA-1 SHA2-256 SHA2-512	N/A	Message digest

The module does not support any non-approved algorithms; therefore, this Security Policy document does not contain tables for “Non-Approved Algorithms Allowed in the Approved Mode of Operation”, “Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed” or “Non-Approved Algorithms Not Allowed in the Approved Mode of Operation”.

Cryptographic boundary

The cryptographic boundary of the CryptoMod module is the cryptomod_fips kernel module of the ONTAP OS kernel. The boundary is depicted in the block diagram below. The approved DRBG is used to supply the module's cryptographic keys. The Tested OE's Physical Perimeter (TOEPP) for the module is the enclosure of the NetApp controller.

Figure 1) Cryptographic boundary and TOEPP



3 Cryptographic module interfaces

As a software-only module, CryptoMod does not have any physical ports, instead, the physical ports are defined as 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 data output interfaces are disabled (note: the module does not utilize control input or output interfaces). Ports and interfaces associated with the module are listed in the table that appears below.

Table 5) Ports and Interfaces

Physical Port	Logical interface	Data that passes over port/interface
Ethernet SATA/SAS/NVMe interfaces	Data passed to the API calls to be used by the module	Data Input
Ethernet SATA/SAS/NVMe interfaces	Data returned by API calls to the module	Data Output
Ethernet	Status data returned by API calls to the module	Status Output

Note: Control input and output interfaces are not implemented by the module

4 Roles, services, and authentication

Roles

The module supports the following roles:

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

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

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.

Services

The module supports services available to users in the available roles. The table that follows shows the available services along with the role, input and output associated with each service.

Table 6) Roles, Service Commands, Input and Output

Role	Service	Input	Output
Crypto-Officer	Show version information	Command and parameters	Command response Return code
Crypto-Officer	Show status	Command and parameters	Command response Return code
Crypto-Officer	Perform on demand self-tests	Performed automatically upon controller reboot	Command response Return code
User	Encryption Decryption	Command and parameters	Command response Return code

Role	Service	Input	Output
User	Authenticated encryption Authenticated decryption	Command and parameters	Command response Return code
User	Key wrapping Key unwrapping	Command and parameters	Command response Return code
User	Random bit generation	Command and parameters	Command response Return code
User	Key generation	Command and parameters	Command response Return code
User	Message authentication	Command and parameters	Command response Return code
User	Hashing	Command and parameters	Command response Return code
User	Key derivation function	Command and parameters	Command response Return code
Crypto-Officer	Zeroize	Reboot	No output returned

The following table identifies the authentication method and strength associated with each role.

Table 7) Roles and Authentication

Role	Authentication Method	Authentication Strength
Crypto-Officer	N/A (Security Level 1)	N/A (Security Level 1)
User	N/A (Security Level 1)	N/A (Security Level 1)

The table below provides a full description of the approved services provided by the module.

Table 8) Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Show version information	Returns the name of the module and the version associated with the module	N/A	N/A	Crypto-Officer	N/A	Output indicates module version number
Show status	Returns the module's status	N/A	N/A	Crypto-Officer	N/A	Output indicates module's status

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Perform on demand self-tests	Initiates and runs the pre-operational self-tests	All	N/A	Crypto-Officer	N/A	Self-tests auto-matically performed when kernel loads module. API output of 0 indicates success.
Encryption Decryption	Perform encryption or decryption using AES	AES-CBC AES-CCM AES-GCM AES-XTS	128- and 256-bit AES keys. Note: XTS mode only with 128- and 256-bit keys.	User	**E, R**, **W**	API output of 0 indicates success
Authenti-cated encryption Authenti-cated Decryption	Perform authenticated encryption or decryption uses AES GCM or AES CCM	AES-CCM AES-GCM	AES-CCM: 128-bit AES keys AES-GCM: 128- and 256-bit AES keys.	User	**E, R**, **W**	API output of 0 indicates success
Key wrapping Key unwrapping	Perform key wrapping or key unwrapping using AES	AES-ECB AES-KWP	128- and 256-bit AES keys	User	**E, R**, **W**	API output of 0 indicates success
Random bit generation	Provide random bits from the module's DRBG	AES-ECB DRBG_CTR	Entropy input string V values Random data	User	**E, G, R**, **W**	API output of 0 indicates success
Key generation	Perform key generation using the module's DRBG	AES-ECB DRBG_CTR	Entropy input string V values Key value	User	**E, G, R**, **W**	API output of 0 indicates success
Message authentic-cation	Perform key hash using HMAC	HMAC-SHA1 HMAC-SHA2-256 HMAC-SHA2-512	160-bit to 512-bit HMAC keys	User	**E, R**, **W**	API output of 0 indicates success

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys and/or SSPs	Indicator
Message authentic-cation	Perform message authentication using AES CMAC or AES GMAC	AES-ECB AES-CMAC	128-bit to 256-bit AES key	User	**E, R**, **W**	API output of 0 indicates success
Hashing	Perform SHA hashing function	SHA-1 SHA2-256 SHA2-512 SHA3-256	N/A	User	N/A	API output of 0 indicates success
Key derivation function	Perform key derivation using PBKDF	PBKDF SHA-1 SHA2-256 SHA2-512	8- to 128-bit passwords 8- to 406-bit keys	User	**E, G, R**, **W**	API output of 0 indicates success
Key derivation function	Perform key derivation using NIST SP800-108 in CTR mode	CKG HMAC-SHA1 HMAC-SHA2-256 HMAC-SHA2-512	8- to 4096-bit keys	User	**E, G, R**, **W**	API output of 0 indicates success
Zeroize	Zeroize keys and CSPs	N/A	All	Crypto-Officer	**Z**	Success-ful comple-tion of reboot operation indicates success

Legend:

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroize: The module zeroizes the SSP.

The cryptographic module does not have the capability of loading software or firmware from an external source.

5 Software/Firmware security

The module compares the HMAC-SHA2-256 digest created over the .text and .data sections of the module versus the digest pre-calculated at compile time. The module's self-integrity check is

automatically performed when the module is loaded into kernel memory. Since the module, once loaded, cannot be unloaded, the self-integrity check can only be initiated by rebooting the platform.

6 Operational environment

The module operates in a modifiable operational environment on the validated platforms listed in Table 2 and the vendor-affirmed platforms listed in Table 3.

7 Physical security

The module is implemented completely in software in such a manner that the physical security is provided solely by the computing platform; therefore, the module is not subject to the physical security requirements.

8 Non-invasive security

The module does not implement non-invasive attack mitigation techniques to protect the module's unprotected SSPs from non-invasive attacks.

9 Sensitive security parameters management

The module supports the following keys and sensitive security parameters (SSPs):

Table 9) SSPs

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Estab-lishment	Storage	Zeroization	Use & related keys
DRBG V value	128-bits	CTR DRBG Cert #A2640	Internally generated	–	–	Non-persistent	Cleared on reboot	DRBG internal state
DRBG internal state key	256-bits	CTR DRBG Cert #A2640	Internally generated	–	–	Non-persistent	Cleared on reboot	DRBG internal state

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Estab-lishment	Storage	Zeroization	Use & related keys
DRBG entropy input string	4096-bits	CTR DRBG Cert #A2640 ESV (#E1)	Internally generated from jitter-entropy noise source	–	–	Non-persistent	Cleared on reboot	DRBG entropy input
DRBG seed	384-bits	CTR DRBG Cert #A2640 ESV (#E1)	Internally generated from jitter-entropy noise source	–	–	Non-persistent	Cleared on reboot	DRBG seed
AES encrypt, decrypt key	128- and 256-bits	AES-EBC AES-CCM AES-CBC AES-GCM AES-XTS Cert #A2640	Generated internally using the approved DRBG or input via API in plaintext	Plaintext electronic import of key for encryption/decryption APIs	Plaintext electronic import	Non-persistent	Cleared on reboot	Sym-metric encryption/decryption.
AES Wrapping /Unwrap-ping Key	128- and 256-bits	AES-EBC AES-KWP Cert #A2640	Generated internally using the Approved DRBG or input via API in plaintext	Plaintext electronic import of key for wrap/unwrap APIs	Plaintext electronic import	Only wrapped keys persistently stored within the storage media	Unwrapped keys cleared on reboot. Wrapped keys deleted when key manager un-configured	Protect plain-text keys

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Estab-lishment	Storage	Zeroization	Use & related keys
AES CCM Key	128-bits	AES-EBC AES-CCM Cert #A2640	Generated internally using the Approved DRBG or input via API in plaintext	Plaintext electronic import of key for encryption/decryption APIs	Plaintext electronic import	Non-persistent	Cleared on reboot	Sym-metric encryption/decryption.
AES GCM Key	128- and 256-bits	Cert #A2640	Generated internally using the Approved DRBG or input via API in plaintext	Plaintext electronic import of key for encryption/decryption APIs	Plaintext electronic import	Non-persistent	Cleared on reboot	Sym-metric encryption/decryption.
AES GCM IV	96-bits	Cert #A2640	Generated externally by the calling application	Plaintext electronic import of IV for encryption/decryption APIs	Plaintext electronic import	Non-persistent	Cleared on reboot	Sym-metric encryption/decryption.
AES XTS Key	128- and 256-bits	Cert #A2640	Generated internally using the Approved DRBG or input via API in plaintext	Plaintext electronic import of key for encryption/decryption APIs	Plaintext electronic import	Non-persistent	Cleared on reboot	Sym-metric encryption/decryption.
HMAC Key	160-, 224-, 256-, 384-, and 512-bits	Cert #A2640	Input via API in plaintext	Plaintext electronic import of key for HMAC APIs	Plaintext electronic import	Non-persistent	Cleared on reboot	Auth-enticated message digest
CPKEK Key	256-bits	Cert #A2640	Derived via PBKDF from a passphrase input via API in plaintext	Plaintext electronic export of key	Plaintext electronic import	Non-persistent	Cleared on reboot	Protect plain-text keys
KDK Key	256-bits	Cert #A2640	Input via API in plaintext	Plaintext electronic import of KDK for APIs	Plaintext electronic import	Non-persistent	Cleared on reboot	Derive additional keys

Key/ SSP Name/ Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Estab-lishment	Storage	Zeroization	Use & related keys
KDK Output Key	256-bits	Cert #A2640	Derived via KDF from the KDK key input via API in plaintext	Plaintext electronic export of derived key	–	Non-persistent	Cleared on reboot	Protect plain-text keys

Key Generation

CryptoMod implements a NIST SP800-90Arev1 DRBG for the generation of random bits and keys. The implementation of the 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 module's embedded jitter-entropy CPU ESV(#E1) implementation. The module uses its embedded entropy source in accordance with the ESV(#E1) Public Use Document. The module requests a minimum number of 512 bits of entropy from its Operational Environment per each call.

In addition, the vendor affirmed CKG implementation uses an Approved counter DRBG as specified in NIST SP800-90Arev1. The key generation method adheres to NIST SP800-133rev2 and the module utilizes post processing. The output of the CryptoMod DRBG is XOR'd with a random mask obtained from ESV (#E1) to compute the secret value "K" as per Section 6.3, method #2 in NIST SP800-133rev2 with m = 1 and n = 1. The post-processing is performed on the DRBG output with the post-processing operation resulting in the new "U".

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.

Key Import/Export

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.

Zeroization Procedures

Keys can be zeroized (overwritten with "zeroes") by rebooting the host NetApp controller.

ESV (#E1)

The ESV (#E1) entropy source used by the CTR_DRBG in the module is described in the following tables.

The module's embedded entropy source provides 256 bits of min-entropy per 256-bit output sample of full entropy.

Table 10) Entropy Certificates

Vendor Name	Certificate
NetApp, Inc	ESV (Cert #E1)

Table 11) Entropy Sources

Name	Type	Operating Environment	Sample Size	Entropy per Sample	Conditioning Component
CPU Jitter RNG v3.4.0	Non-physical	ONTAP 9.11.1 running on Intel Xeon D-2164IT ONTAP 9.11.1 running on Intel Xeon Silver 4210 ONTAP 9.11.1 running on Intel Xeon Platinum 8352Y	64	1	A2640 (SHA3-256)

10 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 140-3 fall within two categories:

1. Pre-operational self-tests, which include:
    a. Software integrity test: the stored HMAC-SHA2-256 values over the .text and .data sections are checked by the module at power-up. This test is performed after the HMAC-SHA2-256 KAT has been performed.
2. Conditional self-tests, which include:
    a. Known Answer Test (KATs) 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
        - AES CMAC for 128 and 256-bit keys

- AES GMAC for 128 and 256-bit keys
- AES XTS encrypt and decrypt for 128 and 256-bit keys
- CTR_DRBG
- HMAC-SHA-1
- HMAC-SHA2-256
- HMAC-SHA2-512
- SP800-108 KDF in CTR mode
- PBKDF
- SHA-1
- SHA2-256
- SHA2-512
- SHA3-256

Since the module is single-threaded, the power-on self-tests need to run to completion before the module can accept cryptographic operation requests from calling applications.

The module performs the following conditional self-tests:

- NIST SP 800-90Arev 1 Section 11 DRBG Health tests; and
- NIST SP 800-90B Section 4.4 RCT and APT health tests.

Per [**SP800-90Arev1**], DRBG conditional self-tests are performed during the power-on self-testing sequence. The entropy source RCT and APT health tests are performed whenever a random value is requested from the entropy source.

If any of the power-up self-tests or conditional tests fail, the module enters a “self-test” error state and ceases operation, inhibiting any further output. The module does not perform any cryptographic operations while it is in an error state. Errors encountered during the power-on self-test operations will result in an automatic reboot of the operating system. If the module encounters a fatal error state, other than one encountered during self-tests, then the Crypto-Officer must manually reboot the system to return the module to normal operation.

11 Life-cycle assurance

The CryptoMod module is automatically installed with ONTAP and is automatically initialized and started up whenever the appliance and/or ONTAP instance is restarted.

See the NetApp documentation center (https://docs.netapp.com) for ONTAP product documentation.

11.1 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 an approved mode of operation.

11.2 Initialization

ONTAP 9.15.1 will use the NetApp CryptoMod version 3.0 module without any required user intervention.

When used with ONTAP versions less than ONTAP 9.15.1, the FIPS 140-3 variant of the module is initialized by executing the following ONTAP CLI diagnostic level command:

```
*> security cryptomod_fips modify -node local -is_iut_enabled true
```

followed by a reboot of the controller. Once the controller has rebooted, the FIPS 140-3 variant of the module will be automatically used.

11.3 User guidance

ONTAP 9.15.1 will use the NetApp CryptoMod version 3.0 module without any required user intervention.

To use the FIPS 140-3 validated variant of the module with ONTAP versions less than 9.15.1, a user needs to run the following ONTAP diagnostic-level command:

```
*> security cryptomod-fips modify -node local -is-iut-enabled true
```

After rebooting the node, the controller will automatically load the FIPS 140-3 validated variant of the module. The FIPS 140-3 validated variant of the module will continue to be used until the user deselects the FIPS 140-3 validated variant of the module by running the following ONTAP CLI diagnostic-level command:

```
*> security cryptomod-fips modify -node local -is-iut-enabled false
```

followed by a reboot of the controller.

Users can determine if they are using the FIPS 140-3 variant of the module by running the following ONTAP CLI command:

```
*> security cryptomod-fips show
```

11.3.1 PBKDF usage guidance

The module provides password-based key derivation (PBKD), compliant with NIST SP 800-132rev2. The CryptoMod module supports option 1a from section 5.4 of **[SP800-132]**. In option 1a, the Master Key (MK), or a segment of the MK, is used directly as the Data Protection Key (DPK).

In line with the requirements for NIST SP800-132, keys generated using the approved PBKDF algorithm must only be used for storage applications. The length of the MK or DPK shall be 112 bits or more.

A salt, with a length of at least 128 bits, shall be generated using the NIST SP 800-90Arev1 DRBG.

The iteration count shall be selected as large as possible, with a minimum value of 1000.

Passwords or passphrases, used as input for the PBKDF, shall not be used as cryptographic keys.

The length of the password of passphrase shall be at least 32 characters and shall consist of ASCII printable characters. The probability of guessing the value is estimated to be:

$1/95^{32} < 10^{-64}$, which is less than 2^{-112}.

As the module is a general-purpose software module, it is not possible to predict the use of the PBKDF, however a user of the module should also note that a password should contain at least enough entropy to be unguessable and contain enough entropy to reflect the security strength required for the key being generated. Users are referred to Appendix A, “Security Considerations” of NIST SP800-132rev2 for further information on password selection.

11.3.2 AES GCM usage guidance

The AES-GCM IV is partially generated by an industry protocol and is always passed to the module via an API call. The counter portion of the IV is set by the module within the module's cryptographic boundary.

When used with TLS 1.2/1.3 the AES-GCM IV is constructed in compliance with IG C.H scenario 1. The GCM IV generation follows RFC 5288. The counter portion of the IV is set by the module within the module's cryptographic boundary. The module does not implement the TLS protocol. The module's implementation of AES-GCM, when used for TLS, is used with another ONTAP application running outside of the module's boundary. The design of the TLS protocol implicitly ensures that the counter portion of the IV will not exhaust all of its possible values.

When used with the IPsec-v3 protocol, GCM IV generation follows RFC 4106 and is constructed in compliance with IG C.H scenario 2. The counter portion of the IV is set by the module within the module's cryptographic boundary. The module does not implement the IPsec protocol. The module's implementation of AES-GCM, when used for IPsec, is used with another ONTAP application running outside of the module's boundary. The design of the IPsec protocol implicitly ensures that the counter portion of the IV will not exhaust all of its possible values.

When used with SMB 3.x, the AES-GCM IV is constructed in compliance with IG C.H scenario 5 with 8 bytes of random data followed by 8 bytes from the network context. The counter portion of the IV is set by the module within the module's cryptographic boundary. The module does not implement the SMB protocol. The module's implementation of AES-GCM, when used for SMB, is used with another ONTAP application running outside of the module's boundary. The design of the SMB protocol implicitly ensures that the counter portion of the IV will not exhaust all of its possible values.

In all instances, the AES-GCM IV is not persistently stored; therefore, whenever the module's power is lost and then restored, the user of the module (i.e., TLS, IPsec, or SMB) along with the ONTAP application that implements the protocol, must re-establish keying material using new random values and KDF operation to establish the pertinent network communication channel.

11.3.3 AES XTS usage guidance

Per the requirements of SP800-38E, AES-XTS mode shall be used for storage purposes only. The length of the AES-XTS data unit does not exceed 2^{20} blocks. In accordance with IG C.I when generating an AES-XTS key, the module checks to ensure that key_1 is not equal to key_2. If key_1 is equal to key_2, then the module fails the key generation request.

12 Mitigation of other attacks

This section is not applicable. The module does not claim to mitigate against any attacks beyond the FIPS 140-3 requirements for a Level 1 module.

Appendix A: Acronyms

This section describes the acronyms used throughout the document.

Table 12) Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
AES-NI	AES New Instructions
AFF	All Flash FAS
API	Application Programming Interface
APT	Adaptive Proportion Test
ASCII	American Standard Code for Information Interchange
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining-Message authentication code
CKG	Cryptographic Key Generation
CLI	Command Line Interface
CPKEK	Cluster Passphrase Key Encryption Key
CPU	Central Processing Unit
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ESV	Entropy Source Validation
FAS	Fabric-Attached Storage
FIPS	Federal Information Processing Standard
GCM	Galois/Counter Mode
GMAC	Galois/counter mode Message Authentication Code
HMAC	Hash Message Authentication Code
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IV	Initialization Vector
KAT	Known Answer Test
KDK	Key Derivation Key
KEK	Key Encryption Key
KTS	Key Transport Scheme

Acronym	Definition
KWP	Key Wrap with Padding
MK	Master Key
NIST	National Institute of Science and Technology
NVMe	Non-Volatile Memory Express
OE	Operational Environment
OS	Operating System
PAA	Processor Algorithm Accelerator
PBKDF	Password Based Key Derivation Function
RCT	Repetition Count Test
SAS	Serial Attached SCSI
SATA	Serial AT Attachment
SCSI	Small Computer System Interface
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SSP	Sensitive Security Parameter
TOEPP	Tested OE's Physical Perimeter
XOR	E**xc**lusive-**OR**
XTS	**X**EX **T**weakable Block Cipher with Ciphertext **S**tealing

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

[FIPS 202] SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

[ISO/IEC 24759] Information technology – Security techniques – Test requirements for cryptographic modules

[SP800-38A] 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

[SP800-38B] NIST Special Publication 800-38B – Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

[SP800-38C] 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

[SP800-38D] 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

[SP800-38E] 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

[SP800-38F] 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

[SP800-90Arev1] 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

[SP800-108] NIST Special Publication 800-108 (Revised) – Recommendation for Key Derivation Using Pseudorandom Functions
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf

[SP800-132] NIST Special Publication 800-132 – Recommendation for Password-Based Key Derivation; Part 1: Storage Applications
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-132.pdf

[SP800-133rev2] NIST Special Publication 800-133 Revision 2 – Recommendation for Cryptographic Key Generation
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf