NetApp, Inc.

NetApp CryptoMod

FIPS 140-3 Non-Proprietary Security Policy

Document Version 1.3

June 2026

NetApp®

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

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:

1.2 Security Levels

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	N/A
9	Sensitive security parameter management	1
10	Self-tests	1
11	Life-cycle assurance	1
12	Mitigation of other attacks	N/A
	Overall Level	1

Table 1: Security Levels

1.3 Additional Information

In accordance with AS02.05, [ISO 19790] §7.7 *Physical Security* is optional and does not apply to the Module. In accordance with current CMVP policy, [ISO 19790] §7.8 *Non-Invasive Security* is not applicable.

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Module is a kernel mode cryptographic software library providing a C-language application program interface (API) for use by ONTAP kernel modules that require cryptographic functionality. The Module is designated as a software module with multi-chip standalone embodiment based on the descriptions of [ISO 19790] AS02.03. The Module is intended for use by US and Canadian Federal agencies and other markets that require FIPS 140-3 validated cryptographic functionality.

The Module’s formal name and version are “CryptoMod” and “3.0”, respectively.

The Module's design corresponds to the Module security roles. Security roles enforced by the Module are described in the appropriate context of the document.

Module Type: Software

Module Embodiment: Multi-Chip Standalone

Cryptographic Boundary:

The cryptographic boundary of the CryptoMod module is the cryptomod_fips kernel module of the ONTAP OS kernel. The cryptographic boundary is depicted in red in the figure below. The Module's approved DRBG is used to supply the Module's cryptographic keys.

Tested Operational Environment's Physical Perimeter (TOEPP):

The Tested OE's Physical Perimeter (TOEPP) for the module is the enclosure of the NetApp controller.

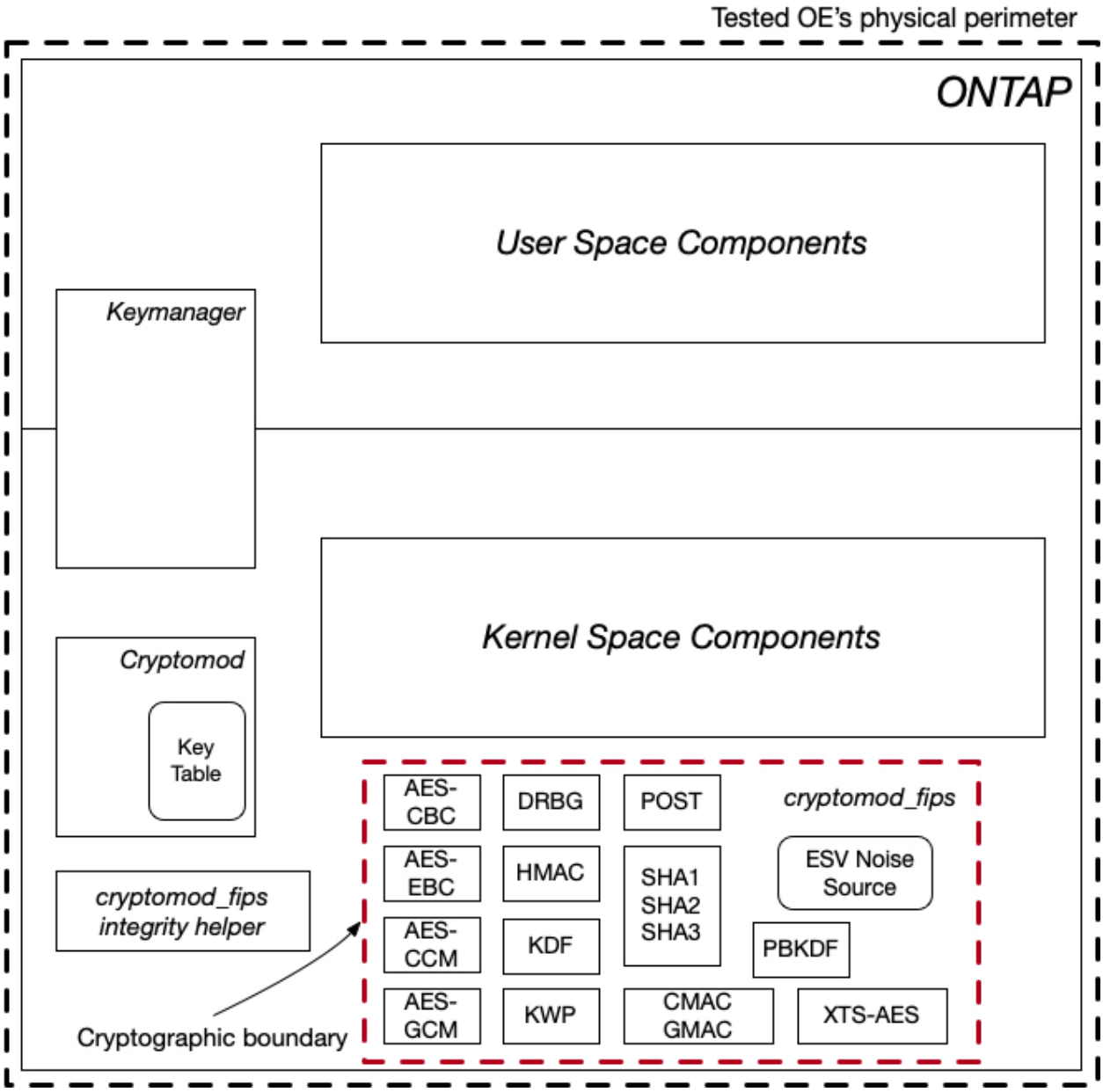

Figure 1: Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

N/A for this module.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

Package or File Name	Software/ Firmware Version	Features	Integrity Test
cryptomod_fips.ko	3.0	N/A	HMAC-SHA2-256

Table 2: Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets)

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform	Processors	PAA/PAI	Hypervisor or Host OS	Version(s)
ONTAP 9.11.1	AFF A250	Intel Xeon D-2164IT	No	N/A	3.0
ONTAP 9.11.1	AFF A250	Intel Xeon D-2164IT	Yes	N/A	3.0
ONTAP 9.11.1	AFF A400	Intel Xeon Silver 4210	No	N/A	3.0
ONTAP 9.11.1	AFF A400	Intel Xeon Silver 4210	Yes	N/A	3.0
ONTAP 9.11.1	AFF A900	Intel Xeon Platinum 8352Y	No	N/A	3.0
ONTAP 9.11.1	AFF A900	Intel Xeon Platinum 8352Y	Yes	N/A	3.0

Table 3: Tested Operational Environments - Software, Firmware, Hybrid

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

Operating System	Hardware Platform
ONTAP 9.11	AFF A150
ONTAP 9.12	AFF A150
ONTAP 9.13	AFF A150
ONTAP 9.14	AFF A150
ONTAP 9.15	AFF A150
ONTAP 9.16	AFF A150
ONTAP 9.17	AFF A150
ONTAP 9.18	AFF A150
ONTAP 9.19	AFF A150
ONTAP 9.15	AFF A1K
ONTAP 9.16	AFF A1K
ONTAP 9.17	AFF A1K
ONTAP 9.18	AFF A1K
ONTAP 9.19	AFF A1K
ONTAP 9.11	AFF A220
ONTAP 9.12	AFF A220
ONTAP 9.13	AFF A220
ONTAP 9.14	AFF A220
ONTAP 9.15	AFF A220
ONTAP 9.16	AFF A220
ONTAP 9.17	AFF A220

Operating System	Hardware Platform
ONTAP 9.18	AFF A220
ONTAP 9.19	AFF A220
ONTAP 9.12	AFF A250
ONTAP 9.13	AFF A250
ONTAP 9.14	AFF A250
ONTAP 9.15	AFF A250
ONTAP 9.16	AFF A250
ONTAP 9.17	AFF A250
ONTAP 9.18	AFF A250
ONTAP 9.19	AFF A250
ONTAP 9.11	AFF A300
ONTAP 9.12	AFF A300
ONTAP 9.13	AFF A300
ONTAP 9.14	AFF A300
ONTAP 9.15	AFF A300
ONTAP 9.16	AFF A300
ONTAP 9.11	AFF A320
ONTAP 9.12	AFF A320
ONTAP 9.13	AFF A320
ONTAP 9.14	AFF A320
ONTAP 9.12	AFF A400
ONTAP 9.13	AFF A400
ONTAP 9.14	AFF A400
ONTAP 9.15	AFF A400
ONTAP 9.16	AFF A400
ONTAP 9.17	AFF A400
ONTAP 9.18	AFF A400
ONTAP 9.19	AFF A400
ONTAP 9.16	AFF A20
ONTAP 9.17	AFF A20
ONTAP 9.18	AFF A20
ONTAP 9.19	AFF A20
ONTAP 9.16	AFF A30
ONTAP 9.17	AFF A30
ONTAP 9.18	AFF A30
ONTAP 9.19	AFF A30
ONTAP 9.16	AFF A50
ONTAP 9.17	AFF A50
ONTAP 9.18	AFF A50
ONTAP 9.19	AFF A50
ONTAP 9.15	AFF A70
ONTAP 9.16	AFF A70
ONTAP 9.17	AFF A70
ONTAP 9.18	AFF A70
ONTAP 9.19	AFF A70
ONTAP 9.15	AFF A90 [1]
ONTAP 9.16	AFF A90 [1]
ONTAP 9.17	AFF A90 [1]

Operating System	Hardware Platform
ONTAP 9.18	AFF A90 [1]
ONTAP 9.19	AFF A90 [1]
ONTAP 9.17	AFF A90M [1]
ONTAP 9.18	AFF A90M [1]
ONTAP 9.19	AFF A90M [1]
ONTAP 9.11	AFF A700
ONTAP 9.12	AFF A700
ONTAP 9.13	AFF A700
ONTAP 9.14	AFF A700
ONTAP 9.15	AFF A700
ONTAP 9.16	AFF A700
ONTAP 9.17	AFF A700
ONTAP 9.18	AFF A700
ONTAP 9.11	AFF A800
ONTAP 9.12	AFF A800
ONTAP 9.13	AFF A800
ONTAP 9.14	AFF A800
ONTAP 9.15	AFF A800
ONTAP 9.16	AFF A800
ONTAP 9.17	AFF A800
ONTAP 9.18	AFF A800
ONTAP 9.19	AFF A800
ONTAP 9.12	AFF A900
ONTAP 9.13	AFF A900
ONTAP 9.14	AFF A900
ONTAP 9.15	AFF A900
ONTAP 9.16	AFF A900
ONTAP 9.17	AFF A900
ONTAP 9.18	AFF A900
ONTAP 9.19	AFF A900
ONTAP 9.16	AFF C30 [1]
ONTAP 9.17	AFF C30 [1]
ONTAP 9.18	AFF C30 [1]
ONTAP 9.19	AFF C30 [1]
ONTAP 9.16	AFF C30 r2
ONTAP 9.17	AFF C30 r2
ONTAP 9.18	AFF C30 r2
ONTAP 9.19	AFF C30 r2
ONTAP 9.16	AFF C60
ONTAP 9.17	AFF C60
ONTAP 9.18	AFF C60
ONTAP 9.19	AFF C60
ONTAP 9.16	AFF C60 r2
ONTAP 9.17	AFF C60 r2
ONTAP 9.18	AFF C60 r2
ONTAP 9.19	AFF C60 r2
ONTAP 9.16	AFF C80
ONTAP 9.17	AFF C80

Operating System	Hardware Platform
ONTAP 9.18	AFF C80
ONTAP 9.19	AFF C80
ONTAP 9.16	AFF C80 r2
ONTAP 9.17	AFF C80 r2
ONTAP 9.18	AFF C80 r2
ONTAP 9.19	AFF C80 r2
ONTAP 9.11	AFF C190
ONTAP 9.12	AFF C190
ONTAP 9.13	AFF C190
ONTAP 9.14	AFF C190
ONTAP 9.15	AFF C190
ONTAP 9.16	AFF C190
ONTAP 9.17	AFF C190
ONTAP 9.18	AFF C190
ONTAP 9.19	AFF C190
ONTAP 9.11	AFF C250
ONTAP 9.12	AFF C250
ONTAP 9.13	AFF C250
ONTAP 9.14	AFF C250
ONTAP 9.15	AFF C250
ONTAP 9.16	AFF C250
ONTAP 9.17	AFF C250
ONTAP 9.18	AFF C250
ONTAP 9.19	AFF C250
ONTAP 9.11	AFF C400
ONTAP 9.12	AFF C400
ONTAP 9.13	AFF C400
ONTAP 9.14	AFF C400
ONTAP 9.15	AFF C400
ONTAP 9.16	AFF C400
ONTAP 9.17	AFF C400
ONTAP 9.18	AFF C400
ONTAP 9.19	AFF C400
ONTAP 9.11	AFF C800
ONTAP 9.12	AFF C800
ONTAP 9.13	AFF C800
ONTAP 9.14	AFF C800
ONTAP 9.15	AFF C800
ONTAP 9.16	AFF C800
ONTAP 9.17	AFF C800
ONTAP 9.18	AFF C800
ONTAP 9.19	AFF C800
ONTAP 9.17	AFX 1K
ONTAP 9.18	AFX 1K
ONTAP 9.19	AFX 1K
ONTAP 9.19	AFX 2K [1]
ONTAP 9.16	ASA A1K
ONTAP 9.17	ASA A1K

Operating System	Hardware Platform
ONTAP 9.18	ASA A1K
ONTAP 9.19	ASA A1K
ONTAP 9.16	ASA A20
ONTAP 9.17	ASA A20
ONTAP 9.18	ASA A20
ONTAP 9.19	ASA A20
ONTAP 9.16	ASA A30
ONTAP 9.17	ASA A30
ONTAP 9.18	ASA A30
ONTAP 9.19	ASA A30
ONTAP 9.16	ASA A50
ONTAP 9.17	ASA A50
ONTAP 9.18	ASA A50
ONTAP 9.19	ASA A50
ONTAP 9.16	ASA A70
ONTAP 9.17	ASA A70
ONTAP 9.18	ASA A70
ONTAP 9.19	ASA A70
ONTAP 9.16	ASA A90 [1]
ONTAP 9.17	ASA A90 [1]
ONTAP 9.18	ASA A90 [1]
ONTAP 9.19	ASA A90 [1]
ONTAP 9.13	ASA A150
ONTAP 9.14	ASA A150
ONTAP 9.15	ASA A150
ONTAP 9.16	ASA A150
ONTAP 9.17	ASA A150
ONTAP 9.18	ASA A150
ONTAP 9.19	ASA A150
ONTAP 9.13	ASA A250
ONTAP 9.14	ASA A250
ONTAP 9.15	ASA A250
ONTAP 9.16	ASA A250
ONTAP 9.17	ASA A250
ONTAP 9.18	ASA A250
ONTAP 9.19	ASA A250
ONTAP 9.13	ASA A400
ONTAP 9.14	ASA A400
ONTAP 9.15	ASA A400
ONTAP 9.16	ASA A400
ONTAP 9.17	ASA A400
ONTAP 9.18	ASA A400
ONTAP 9.19	ASA A400
ONTAP 9.13	ASA A800
ONTAP 9.14	ASA A800
ONTAP 9.15	ASA A800
ONTAP 9.16	ASA A800
ONTAP 9.17	ASA A800

Operating System	Hardware Platform
ONTAP 9.18	ASA A800
ONTAP 9.19	ASA A800
ONTAP 9.13	ASA A900
ONTAP 9.14	ASA A900
ONTAP 9.15	ASA A900
ONTAP 9.16	ASA A900
ONTAP 9.17	ASA A900
ONTAP 9.18	ASA A900
ONTAP 9.19	ASA A900
ONTAP 9.11	ASA AFF A220
ONTAP 9.12	ASA AFF A220
ONTAP 9.13	ASA AFF A220
ONTAP 9.14	ASA AFF A220
ONTAP 9.15	ASA AFF A220
ONTAP 9.16	ASA AFF A220
ONTAP 9.17	ASA AFF A220
ONTAP 9.18	ASA AFF A220
ONTAP 9.19	ASA AFF A220
ONTAP 9.11	ASA AFF A250
ONTAP 9.12	ASA AFF A250
ONTAP 9.13	ASA AFF A250
ONTAP 9.11	ASA AFF A400
ONTAP 9.12	ASA AFF A400
ONTAP 9.13	ASA AFF A400
ONTAP 9.11	ASA AFF A700
ONTAP 9.12	ASA AFF A700
ONTAP 9.13	ASA AFF A700
ONTAP 9.14	ASA AFF A700
ONTAP 9.15	ASA AFF A700
ONTAP 9.16	ASA AFF A700
ONTAP 9.17	ASA AFF A700
ONTAP 9.18	ASA AFF A700
ONTAP 9.11	ASA AFF A800
ONTAP 9.12	ASA AFF A800
ONTAP 9.13	ASA AFF A800
ONTAP 9.16	ASA C30
ONTAP 9.17	ASA C30
ONTAP 9.18	ASA C30
ONTAP 9.19	ASA C30
ONTAP 9.13	ASA C250
ONTAP 9.14	ASA C250
ONTAP 9.15	ASA C250
ONTAP 9.16	ASA C250
ONTAP 9.17	ASA C250
ONTAP 9.18	ASA C250
ONTAP 9.19	ASA C250
ONTAP 9.13	ASA C400
ONTAP 9.14	ASA C400

Operating System	Hardware Platform
ONTAP 9.15	ASA C400
ONTAP 9.16	ASA C400
ONTAP 9.17	ASA C400
ONTAP 9.18	ASA C400
ONTAP 9.19	ASA C400
ONTAP 9.13	ASA C800
ONTAP 9.14	ASA C800
ONTAP 9.15	ASA C800
ONTAP 9.16	ASA C800
ONTAP 9.17	ASA C800
ONTAP 9.18	ASA C800
ONTAP 9.19	ASA C800
ONTAP 9.16	FAS50
ONTAP 9.17	FAS50
ONTAP 9.18	FAS50
ONTAP 9.19	FAS50
ONTAP 9.15	FAS70
ONTAP 9.16	FAS70
ONTAP 9.17	FAS70
ONTAP 9.18	FAS70
ONTAP 9.19	FAS70
ONTAP 9.15	FAS90 [1]
ONTAP 9.16	FAS90 [1]
ONTAP 9.17	FAS90 [1]
ONTAP 9.18	FAS90 [1]
ONTAP 9.19	FAS90 [1]
ONTAP 9.11	FAS2720
ONTAP 9.12	FAS2720
ONTAP 9.13	FAS2720
ONTAP 9.14	FAS2720
ONTAP 9.15	FAS2720
ONTAP 9.16	FAS2720
ONTAP 9.17	FAS2720
ONTAP 9.18	FAS2720
ONTAP 9.19	FAS2720
ONTAP 9.11	FAS2750
ONTAP 9.12	FAS2750
ONTAP 9.13	FAS2750
ONTAP 9.14	FAS2750
ONTAP 9.15	FAS2750
ONTAP 9.16	FAS2750
ONTAP 9.17	FAS2750
ONTAP 9.18	FAS2750
ONTAP 9.19	FAS2750
ONTAP 9.13	FAS2820
ONTAP 9.14	FAS2820
ONTAP 9.15	FAS2820
ONTAP 9.16	FAS2820

Operating System	Hardware Platform
ONTAP 9.17	FAS2820
ONTAP 9.18	FAS2820
ONTAP 9.19	FAS2820
ONTAP 9.11	FAS500f
ONTAP 9.12	FAS500f
ONTAP 9.13	FAS500f
ONTAP 9.14	FAS500f
ONTAP 9.15	FAS500f
ONTAP 9.16	FAS500f
ONTAP 9.17	FAS500f
ONTAP 9.18	FAS500f
ONTAP 9.11	FAS8200
ONTAP 9.12	FAS8200
ONTAP 9.13	FAS8200
ONTAP 9.14	FAS8200
ONTAP 9.15	FAS8200
ONTAP 9.16	FAS8200
ONTAP 9.11	FAS8300
ONTAP 9.12	FAS8300
ONTAP 9.13	FAS8300
ONTAP 9.14	FAS8300
ONTAP 9.15	FAS8300
ONTAP 9.16	FAS8300
ONTAP 9.17	FAS8300
ONTAP 9.18	FAS8300
ONTAP 9.19	FAS8300
ONTAP 9.11	FAS8700
ONTAP 9.12	FAS8700
ONTAP 9.13	FAS8700
ONTAP 9.14	FAS8700
ONTAP 9.15	FAS8700
ONTAP 9.16	FAS8700
ONTAP 9.17	FAS8700
ONTAP 9.18	FAS8700
ONTAP 9.19	FAS8700
ONTAP 9.11	FAS9000
ONTAP 9.12	FAS9000
ONTAP 9.13	FAS9000
ONTAP 9.14	FAS9000
ONTAP 9.15	FAS9000
ONTAP 9.16	FAS9000
ONTAP 9.17	FAS9000
ONTAP 9.18	FAS9000
ONTAP 9.11	FAS9500
ONTAP 9.12	FAS9500
ONTAP 9.13	FAS9500
ONTAP 9.14	FAS9500
ONTAP 9.15	FAS9500

Operating System	Hardware Platform
ONTAP 9.16	FAS9500
ONTAP 9.17	FAS9500
ONTAP 9.18	FAS9500
ONTAP 9.19	FAS9500
ONTAP 9.11	AFF A700s [2]
ONTAP 9.12	AFF A700s [2]
ONTAP 9.13	AFF A700s [2]
ONTAP 9.14	AFF A700s [2]
ONTAP 9.15	AFF A700s [2]
ONTAP 9.16	AFF A700s [2]
ONTAP 9.17	AFF A700s [2]
ONTAP 9.18	AFF A700s [2]
ONTAP 9.19	AFF A700s [2]
Data ONTAP Select 9.11 with VMware ESXi 7, 8	FDvM300-16GB
Data ONTAP Select 9.12 with VMware ESXi 7, 8	FDvM300-16GB
Data ONTAP Select 9.13 with VMware ESXi 7, 8	FDvM300-16GB
Data ONTAP Select 9.14 with VMware ESXi 7, 8	FDvM300-16GB
Data ONTAP Select 9.15 with VMware ESXi 7, 8	FDvM300-16GB
Data ONTAP Select 9.16 with VMware ESXi 7, 8	FDvM300-16GB
Data ONTAP Select 9.17 with VMware ESXi 7, 8, 9	FDvM300-16GB
Data ONTAP Select 9.18 with VMware ESXi 7, 8, 9	FDvM300-16GB
Data ONTAP Select 9.19 with VMware ESXi 8, 9	FDvM300-16GB
Data ONTAP Select 9.14 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4	FDvM300-16GB
Data ONTAP Select 9.15 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4	FDvM300-16GB
Data ONTAP Select 9.16 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6	FDvM300-16GB
Data ONTAP Select 9.17 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 10	FDvM300-16GB
Data ONTAP Select 9.18 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 10, 10.1	FDvM300-16GB
Data ONTAP Select 9.19 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 10, 10.1	FDvM300-16GB
Data ONTAP Select 9.11 with VMware ESXi 7, 8	FDvM300-64GB
Data ONTAP Select 9.12 with VMware ESXi 7, 8	FDvM300-64GB
Data ONTAP Select 9.13 with VMware ESXi 7, 8	FDvM300-64GB
Data ONTAP Select 9.14 with VMware ESXi 7, 8	FDvM300-64GB
Data ONTAP Select 9.15 with VMware ESXi 7, 8	FDvM300-64GB
Data ONTAP Select 9.16 with VMware ESXi 7, 8	FDvM300-64GB
Data ONTAP Select 9.17 with VMware ESXi 7, 8, 9	FDvM300-64GB
Data ONTAP Select 9.18 with VMware ESXi 7, 8, 9	FDvM300-64GB
Data ONTAP Select 9.19 with VMware ESXi 8, 9	FDvM300-64GB
Data ONTAP Select 9.14 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4	FDvM300-64GB
Data ONTAP Select 9.15 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4	FDvM300-64GB

Operating System	Hardware Platform
Data ONTAP Select 9.16 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5. 9.6	FDvM300-64GB
Data ONTAP Select 9.17 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 10	FDvM300-64GB
Data ONTAP Select 9.18 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 10, 10.1	FDvM300-64GB
Data ONTAP Select 9.19 with RHEL Server KVM 8.6, 8.7, 8.8, 8.9, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 10, 10.1	FDvM300-64GB
Data ONTAP Select 9.11 with VMware ESXi 7, 8	FDvM300-128GB
Data ONTAP Select 9.12 with VMware ESXi 7, 8	FDvM300-128GB
Data ONTAP Select 9.13 with VMware ESXi 7, 8	FDvM300-128GB
Data ONTAP Select 9.14 with VMware ESXi 7, 8	FDvM300-128GB
Data ONTAP Select 9.15 with VMware ESXi 7, 8	FDvM300-128GB
Data ONTAP Select 9.16 with VMware ESXi 7, 8	FDvM300-128GB
Data ONTAP Select 9.17 with VMware ESXi 7, 8, 9	FDvM300-128GB
Data ONTAP Select 9.18 with VMware ESXi 7, 8, 9	FDvM300-128GB
Data ONTAP Select 9.19 with VMware ESXi 8, 9	FDvM300-128GB
Amazon FSx for NetApp ONTAP 9.11	AWS EC2 Nitro [3]
Amazon FSx for NetApp ONTAP 9.12	AWS EC2 Nitro [3]
Amazon FSx for NetApp ONTAP 9.13	AWS EC2 Nitro [3]
Amazon FSx for NetApp ONTAP 9.14	AWS EC2 Nitro [3]
Amazon FSx for NetApp ONTAP 9.15	AWS EC2 Nitro [3]
Amazon FSx for NetApp ONTAP 9.16	AWS EC2 Nitro [3]
Amazon FSx for NetApp ONTAP 9.17	AWS EC2 Nitro [3]
Amazon FSx for NetApp ONTAP 9.18	AWS EC2 Nitro [3]
Amazon FSx for NetApp ONTAP 9.19	AWS EC2 Nitro [3]
Cloud Volumes ONTAP 9.11	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.12	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.13	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.14	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.15	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.16	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.17	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.18	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.19	Microsoft Azure Compute [4]
Cloud Volumes ONTAP 9.11	Google Compute Engine [5]
Cloud Volumes ONTAP 9.12	Google Compute Engine [5]

Operating System	Hardware Platform
Cloud Volumes ONTAP 9.13	Google Compute Engine [5]
Cloud Volumes ONTAP 9.14	Google Compute Engine [5]
Cloud Volumes ONTAP 9.15	Google Compute Engine [5]
Cloud Volumes ONTAP 9.16	Google Compute Engine [5]
Cloud Volumes ONTAP 9.17	Google Compute Engine [5]
Cloud Volumes ONTAP 9.18	Google Compute Engine [5]
Cloud Volumes ONTAP 9.19	Google Compute Engine [5]

Table 4: Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid

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.

[1] CPU models will vary. See NetApp KB SU512 for more details.
[2] Supported only for NetApp's cloud-based deployments in later ONTAP releases.
[3] See https://docs.aws.amazon.com/us_en/fsx/latest/ONTAPGuide/what-is-fsx-ontap.html
[4] See https://learn.microsoft.com/en-us/azure/azure-netapp-files/
[5] See https://docs.cloud.google.com/netapp/volumes/docs/discover/overview

2.3 Excluded Components

No components are excluded from the [FIPS 140-3] requirements.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved mode	The module must be installed per instructions provided in Section 11 of this document.	Approved	FIPS mode = true

Table 5: Modes List and Description

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.

Mode Change Instructions and Status:

The Module only supports an Approved mode of operation.

Degraded Mode Description:

The Module does not support a degraded mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A2640	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-CCM	A2640	Key Length - 128 Tag Length - 128, 64, 96 IV Length - IV Length: 56-104 Increment 8 Payload Length - Payload Length: 0-256 Increment 8 AAD Length - AAD Length: 0-16384 Increment 8	SP 800-38C
AES-CMAC	A2640	Direction - Generation, Verification Key Length - 128, 256 MAC Length - MAC Length: 32-128 Increment 8 Message Length - Message Length: 0-524288 Increment 8	SP 800-38B
AES-ECB	A2640	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A2640	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 Payload Length - Payload Length: 128, 408, 480, 512 AAD Length - AAD Length: 0, 128, 160, 512, 720	SP 800-38D
AES-GMAC	A2640	Direction - Decrypt, Encrypt IV Generation - External Key Length - 128, 256 Tag Length - 128, 64, 96 IV Length - IV Length: 96 AAD Length - AAD Length: 0-65536 Increment 8	SP 800-38D
AES-KWP	A2640	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 256	SP 800-38F

Algorithm	CAVP Cert	Properties	Reference
		Payload Length - Payload Length: 8-4096 Increment 8	
AES-XTS Testing Revision 2.0	A2640	Direction - Decrypt, Encrypt Key Length - 128, 256 Payload Length - Payload Length: 128-65536 Increment 8 Tweak Mode - Hex Data Unit Length - Data Unit Length: 128-65536 Increment 8 Data Unit Length Matches Payload Length - No	SP 800-38E
Counter DRBG	A2640	Prediction Resistance - Yes Supports Reseed - Yes Mode - AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0-512 Increment 8 Entropy Input - Entropy Input: 256-1024 Increment 8 Nonce - Nonce: 128 Personalization String Length - Personalization String Length: 0-512 Increment 8 Returned Bits - 1024	SP 800-90A Rev. 1
HMAC-SHA-1	A2640	MAC - MAC: 32-160 Increment 8 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A2640	MAC - MAC: 32-256 Increment 8 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A2640	MAC - MAC: 32-512 Increment 8 Key Length - Key Length: 8-524288 Increment 8	FIPS 198-1
KDF SP800-108	A2640	KDF Mode - Counter MAC Mode - HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512 Supported Lengths - Supported Lengths: 8-4096 Increment 8 Fixed Data Order - Before Fixed Data Counter Length - 32 Supports Empty IV - No Custom Key In Length - 0	SP 800-108 Rev. 1
PBKDF	A2640	Iteration Count - Iteration Count: 1000-10000000 Increment 1 HMAC Algorithm - SHA-1, SHA2-256, SHA2-512 Password Length - Password Length: 8-128 Increment 8	SP 800-132

Algorithm	CAVP Cert	Properties	Reference
		Salt Length - Salt Length: 128-4096 Increment 8 Key Data Length - Key Data Length: 112-4096 Increment 8	
SHA-1	A2640	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-256	A2640	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA2-512	A2640	Message Length - Message Length: 0-65536 Increment 8	FIPS 180-4
SHA3-256	A2640	Message Length - Message Length: 0-65536 Increment 8	FIPS 202

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

Name	Properties	Implementation	Reference
CKG - Section 6.3	Key Type:Symmetric	NetApp CryptoMod	SP 800-133 Rev. 2 Section 6.3: Symmetric Keys Produced by Combining Multiple Keys and Other Data. (Method 2)

Table 7: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

The Module does not support any Non-Approved, Allowed Algorithms.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

The Module does not support any Non-Approved, Allowed Algorithms with No Security Claimed.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

The Module does not support any Non-Approved, Not Allowed Algorithms.

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Symmetric Encryption and Decryption	BC-UnAuth	Symmetric encryption and decryption	Key Length:128, 256 bits	AES-CBC: (A2640) AES-ECB: (A2640) AES-XTS Testing Revision 2.0: (A2640)
Authenticated Symmetric Encryption and Decryption	BC-Auth	Authenticated symmetric encryption and decryption	Key Length:128, 256 bits Key Length (CCM):128 bits	AES-CCM: (A2640) AES-CMAC: (A2640) AES-GCM: (A2640) AES-GMAC: (A2640)
Message Digest	SHA	Message Digest	Publication:FIPS 180-4	SHA-1: (A2640) SHA2-256: (A2640) SHA2-512: (A2640) SHA3-256: (A2640)
Keyed Hash	MAC	Keyed Hash	Publication:FIPS 198-1	HMAC-SHA-1: (A2640) HMAC-SHA2-256: (A2640) HMAC-SHA2-512: (A2640)
AES Keyed Hash	BC-Auth MAC	Keyed Hash	Key Length:128, 256 bits Key Length (CCM):128 bits	AES-CMAC: (A2640) AES-GMAC: (A2640)
Random Number Generation	DRBG	Random Number Generation	Publication:SP 800-90A Rev. 1	Counter DRBG: (A2640)
Entropy Noise Source	ENT-Cond ENT-ESV ENT-NP	Entropy noise source	Publication:SP 800-90B	SHA3-256: (A2640)
Cryptographic Key Generation (CKG)	CKG	AES keys generated to comply with the approved key generation guidelines of SP800-133 Rev. 2, Section 6.3, Symmetric Keys Produced by Combining	Key Length:128, 256 bits	SHA3-256: (A2640)

Name	Type	Description	Properties	Algorithms
		Multiple Keys and Other Data		
Key Derivation	KBKDF PBKDF	Derive keying material	Publications:SP 800-108 Rev. 1 UPD 1, SP 800-132 Key size:8 to 4096 bit derived keys	KDF SP800-108: (A2640) PBKDF: (A2640)
KTS-AES	KTS-Wrap	AES keys generated to comply with the approved key generation guidelines of SP800-133 Rev. 2, Section 6.3, Symmetric Keys Produced by Combining Multiple Keys and Other Data	Publication:SP 800-38F Key Strength:Key establishment methodology provides between 128 and 256 bits of encryption strength	AES-KWP: (A2640)
Software Integrity Test	MAC	HMAC-SHA2-256 used to perform the software integrity test	Key size:256 bits	HMAC-SHA2-256: (A2640)
Perform self-tests (All)	BC-Auth BC-UnAuth DRBG KBKDF MAC PBKDF SHA	All self-tests executed by the module at boot		AES-CBC: (A2640) AES-CCM: (A2640) AES-CMAC: (A2640) AES-ECB: (A2640) AES-GCM: (A2640) AES-XTS Testing Revision 2.0: (A2640) Counter DRBG: (A2640) HMAC-SHA-1: (A2640) HMAC-SHA2-256: (A2640) HMAC-SHA2-512: (A2640) KDF SP800-

Name	Type	Description	Properties	Algorithms
				108: (A2640) PBKDF: (A2640) SHA-1: (A2640) SHA2-256: (A2640) SHA2-512: (A2640) SHA3-256: (A2640)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

a) AES-GCM Usage

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 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 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 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 a KDF operation to establish the pertinent network communication channel.

b) PBKDF Usage

The module provides password-based key derivation (PBKD), compliant with NIST SP 800-132 Rev. 2. 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 SP 800-132 Rev. 2 for further information on password selection.

c) AES-XTS Usage

Per the requirements of NIST SP 800-38E, 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.

d) SHA-1 Usage

The module implements SHA-1 for usage in the following:

- As a PRF in the KDF for PBKDF [SP800-132]
- As a standalone SHA-1 hash function
- As a PRF in HMAC-SHA-1

e) FIPS 202 Usage

In accordance with IG C.C Resolution 2.a, each SHA-3 function has been tested and validated on all the module’s operating environments.

2.8 RBG and Entropy

Cert Number	Vendor Name
Entropy Certificate #E1	NetApp, Inc.

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
CPU Jitter RNG v3.4.0	Non-Physical	ONTAP 9.16.1 on Intel® Xeon® Bronze 3508U (Sapphire Rapids), ONTAP 9.16.1 on Intel® Xeon® Gold 6438N (Sapphire Rapids), ONTAP 9.16.1 on Intel® Xeon® Platinum 8352Y (Ice Lake), ONTAP 9.16.1 on Intel® Xeon® D-1735TR (Ice Lake), ONTAP 9.16.1 on Silver 4210 (Cascade Lake), ONTAP 9.16.1 on Intel® Xeon® Silver 4114 (Skylake), ONTAP 9.16.1 on Intel® Xeon® D-2164IT (Skylake), ONTAP 9.16.1 on Intel® Xeon® D-1557 (Broadwell)	64	1	SHA3-256 (A2640)

Table 10: Entropy Sources

The ESV (#E1) entropy source used by the Counter DRBG in the module is described above. The module's embedded entropy source provides 256 bits of min-entropy per 256-bit output sample of full entropy.

2.9 Key Generation

CryptoMod implements a NIST SP800-90A Rev. 1 Counter DRBG for the generation of random bits and keys. The implementation of the Counter 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 SP 800-90 A Rev. 1. The key generation method adheres to NIST SP800-133 Rev. 2, 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 SP800-133 Rev. 2 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".

2.10 Key Establishment

Key Agreement Schemes

The Module does not support any key establishment algorithms.

Key Transport Schemes

The module implements the following Approved/allowed key transport methods as specified in [FIPS140-3_IG] IG D.G which have been CAVP tested and validated:

- AES-KWP wrap/unwrap

2.11 Industry Protocols

The Module conforms to Resolution 3 per [FIPS140-3_IG] D.C References to the Support of Industry Protocols: while it provides cryptographic APIs that may be used by IPSec and TLS components, the Module does not contain an implementation for IPSec or TLS. The following caveat is required:

No parts of the IPSec and TLS protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
N/A	Control Input	API call parameters passed by reference or value for cryptographic service input
N/A	Control Output	Not implemented
N/A	Data Input	API call parameters passed by reference or value for cryptographic service input
N/A	Data Output	API call parameters passed by reference or value for cryptographic service output
N/A	Status Output	API return value: enumerated status resulting from call execution

Table 11: Ports and Interfaces

As a software-only module, CryptoMod does not have any physical ports. 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).

4 Roles, Services, and Authentication

4.1 Authentication Methods

N/A for this module.

The Module does not provide an authentication or identification method of its own; operators implicitly assume an authorized role based on the service selected.

4.2 Roles

Name	Type	Operator Type	Authentication Methods
User	Role	User	
Crypto Officer	Role	Crypto Officer	

Table 12: Roles

The module supports the User and mandatory Cryptographic Officer operational role, which is implicitly defined. The module does not support a maintenance role, nor does it support a bypass capability. The module does not support multiple concurrent operators.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Show versioning information	Returns the name of the module and the version associated with the module	N/A	API call parameters	Module name and version		Crypto Officer
Show status	Return FIPS mode status	FIPS status	API call parameters	FIPS status		Crypto Officer
Perform on demand self-tests	Initiates and runs the pre-operational self-tests	API output of 0 indicates success	API call parameters	API output of 0 indicates success, non-zero indicates failure	Perform self-tests (All) Software Integrity Test	Crypto Officer
Encryption/decryption	Perform encryption or decryption using AES	API output of 0 indicates success	API call parameters	Status return, plaintext or ciphertext	Symmetric Encryption and Decryption	User - AES key: E,W - AES XTS key: E,W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Authenticated encryption/decryption	Perform encryption or decryption using AES CCM or AES GCM	API output of 0 indicates success	API call parameters	Status return, plaintext or ciphertext	Authenticated Symmetric Encryption and Decryption	User - AES CCM key: E,W - AES GCM key: E,W
Key wrapping/unwrapping	Perform key wrapping or unwrapping using AES	API output of 0 indicates success	API call parameters	Status return, wrapped or unwrapped key	KTS-AES	User - AES key: E,R,W - CPKEK key: E,R,W
Random bit generation	Provide random bits from the module's DRBG	API output of 0 indicates success	API call parameters	Status, random bytes	Entropy Noise Source Random Number Generation	User - DRBG V value: E,G - DRBG entropy input: E,G - DRBG internal state key: E,G - ESV state: E,G
Key generation	Perform key generation using the module's DRBG	API output of 0 indicates success	API call parameters	Status return, key	Entropy Noise Source Random Number Generation Cryptographic Key Generation (CKG)	User - AES key: R - AES CCM key: R - AES CMAC key: R - AES GCM key: R - AES GMAC key: R - AES KEK key: R - AES XTS key: R

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
HMAC message authentication	Generate or verify data integrity	API output of 0 indicates success	API call parameters	Status return, tag value	Keyed Hash	User - HMAC key: E,R,W
AES message authentication	Generate or verify data integrity	API output of 0 indicates success	API call parameters	Status return, tag value	AES Keyed Hash	User - AES CCM key: E,R,W - AES GCM key: E,R,W
Hashing	Perform SHA hashing function	API output of 0 indicates success	API call parameters	Status return, digest	Message Digest	User
Key derivation	Perform key derivation using PBKDF or NIST SP 800-108 in CTR mode	API output of 0 indicates success	API call parameters	Status return, key	Key Derivation	User - Passphrase: E,W,Z - CPKEK key: G,R - KDK key: E,W - KDK output key: G,R
Zeroize	Zeroize and deallocate memory containing sensitive data	None	Reboot or power cycle NetApp platform	None		Crypto Officer - AES key: Z - AES CCM key: Z - AES CMAC key: Z - AES GCM key: Z - AES GMAC key: Z - AES KEK key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - AES XTS key: Z - CPKEK key: Z - HMAC key: Z - DRBG V value: Z - DRBG entropy input: Z - DRBG internal state key: Z - DRBG seed: Z - ESV state: Z - KDK key: Z - KDK output key: Z - Passphrase: Z

Table 13: Approved Services

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.

4.4 Non-Approved Services

N/A for this module.

The Module does not support any non-approved services.

4.5 External Software/Firmware Loaded

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

5 Software/Firmware Security

5.1 Integrity Techniques

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.

5.2 Initiate on Demand

The Module does not support initiate on demand functionality. The self-integrity check can only be initiated by rebooting the platform.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Modifiable

How Requirements are Satisfied:

The module operates in a modifiable operational environment on the validated platforms and the vendor-affirmed platforms listed in Section 2.2 Tested and Vendor Affirmed Module Version and Identification. The Module conforms to [FIPS 140-3_IG] 2.3.C Processor Algorithm Accelerators (PAA) and Processor Algorithm Implementation (PAI). The AES-NI functions are identified by [FIPS 140-3_IG] 2.3.C as a known PAA.

6.2 Configuration Settings and Restrictions

No operational environment restrictions are required for operation in the approved mode. As indicated in Section 2, the Module always operates in the approved mode.

7 Physical Security

Physical Security requirements are not applicable for this software Module.

8 Non-Invasive Security

In accordance with current CMVP policy, Non-Invasive Security is not applicable.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
RAM	Temporary, plaintext storage	Dynamic

Table 14: Storage Areas

The cryptographic module does not persistently store 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.

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
[Input] Call stack parameters	Calling application	Module	Plaintext	Manual	Electronic	
[Output] Call stack parameters	Module	Calling application	Plaintext	Manual	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Cleansed	Zeroisation of SSPs managed by the caller	Overwrites with random data followed by an overwrite with zeroes	Module initiated
Cleared after use	Zeroisation of temporary copies of CSPs within the relevant function	Overwrites with zeroes	Module initiated
Reboot	RAM is used for temporary storage of SSPs	Restarting the NetApp controller clears the SSPs in RAM	Operator initiated

Table 16: SSP Zeroization Methods

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
AES key	AES key used for symmetric decryption, encryption	128, 256 bits - 128, 256 bits	Symmetric Key - CSP	Cryptographic Key Generation (CKG)		Symmetric Encryption and Decryption
AES CCM key	AES CCM key used for authenticated symmetric decryption, encryption	128 bits - 128 bits	Symmetric Key - CSP			Authenticated Symmetric Encryption and Decryption
AES CMAC key	AES CMAC key used for CMAC generation, verification	128, 256 bits - 128, 256 bits	MAC - CSP			AES Keyed Hash
AES GCM key	AES GCM key used for authenticated symmetric decryption, encryption	128, 256 bits - 128, 256 bits	Symmetric Key - CSP			Authenticated Symmetric Encryption and Decryption
AES GMAC key	AES GMAC key used for GMAC generation, verification	128, 256 bits - 128, 256 bits	MAC - CSP			AES Keyed Hash
AES KEK key	Key wrapping and unwrapping	128, 256 bits - 128, 256 bits	Symmetric Key - CSP	Cryptographic Key Generation (CKG)		KTS-AES
AES XTS key	AES XTS key used for symmetric	128, 256 bits - 128, 256 bits	Symmetric Key - CSP	Cryptographic Key Generation (CKG)		Symmetric Encryption and Decryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	decryption, encryption					
CPKEK key	Key wrapping and unwrapping	128, 256 bits - 128, 256 bits	Symmetric Key - CSP	Key Derivation		KTS-AES
HMAC key	Keyed Hash	112 bits (minimum) - 112 bits (minimum)	MAC - CSP			Keyed Hash
DRBG V value	State value for DRBG	256 bits - 256 bits	256 bits - CSP	Random Number Generation		Random Number Generation
DRBG entropy input	Entropy material for DRBG	4096 bits - N/A	Entropy input - CSP	Entropy Noise Source		Random Number Generation
DRBG internal state key	DRBG internal state key	256 bits - 256 bits	CTR_DRBG_ Key - CSP	Random Number Generation		
DRBG seed	Seeding material for DRBG	384 bits - 384 bits	Entropy input - CSP	Entropy Noise Source		Random Number Generation
ESV state	ESV internal state	N/A - 256 bits	Entropy state - CSP	Entropy Noise Source		Entropy Noise Source
KDK key	Key derivation source key	256 bits - 256 bits	KDF - CSP			Key Derivation
KDK output key	Key derivation output key	256 bits - 256 bits	KDF - CSP		Key Derivation	
Passphrase	Input to PBKDF for key derivation	32 to 256 bytes - 112 bits or greater	Symmetric Key - CSP			Key Derivation

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
AES key	[Input] Call stack	RAM:Plaintext	Call lifetime	Cleansed Cleared	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	parameters [Output] Call stack parameters			after use Reboot	
AES CCM key	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
AES CMAC key	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
AES GCM key	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
AES GMAC key	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
AES KEK key	[Input] Call stack parameters [Output] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
AES XTS key	[Input] Call stack parameters [Output] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
CPKEK key	[Input] Call stack parameters [Output] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
HMAC key	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
DRBG V value	[Input] Call stack parameters [Output] Call stack parameters	RAM:Plaintext	Module lifetime	Reboot	

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG entropy input	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleared after use Reboot	DRBG seed:Used to derive
DRBG internal state key	[Input] Call stack parameters [Output] Call stack parameters	RAM:Plaintext	Module lifetime	Cleansed Cleared after use Reboot	DRBG seed:Derived from
DRBG seed	[Input] Call stack parameters [Output] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	DRBG entropy input:Derived from
ESV state	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleared after use Reboot	
KDK key	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
KDK output key	[Output] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	
Passphrase	[Input] Call stack parameters	RAM:Plaintext	Call lifetime	Cleansed Cleared after use Reboot	

Table 18: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
HMAC-SHA2-256 (A2640)	Key length: 256 bits	KAT	SW/FW Integrity	Success: all self-tests passed (as expected)	MAC (HMAC-SHA2-256, A2640)

Table 19: Pre-Operational Self-Tests

The module is compliant with FIPS 140-3 IG 10.2.A in that it performs a self-test, a Known Answer Test (KAT) for the HMAC-SHA2-256 algorithm.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC	Key Length: 128 and 256 bits	KAT	CAST	FIPS_OK	Encrypt/Decrypt	On reloading the module
AES-CCM	Key Length: 128 bits	KAT	CAST	FIPS_OK	Encrypt/Decrypt	On reloading the module
AES-CMAC	Key Length: 128 and 256 bits	KAT	CAST	FIPS_OK	Hash	On reloading the module
AES-ECB	Key Length: 128 and 256 bits	KAT	CAST	FIPS_OK	Encrypt/Decrypt	On reloading the module
AES-GCM	Key Length: 128 and 256 bits	KAT	CAST	FIPS_OK	Encrypt/Decrypt	On reloading the module
AES-KWP	Key Length: 128 and 256 bits	KAT	CAST	FIPS_OK	Encrypt/Decrypt	On reloading the module
AES-GMAC	Key Length: 128 and 256 bits	KAT	CAST	FIPS_OK	Encrypt/Decrypt	On reloading the module
AES-XTS Testing Revision 2.0	Key Length: 128 and 256 bits	KAT	CAST	FIPS_OK	Encrypt/Decrypt	On reloading the module
Counter DRBG	AES CTR (256 bits) with derivation function	KAT	CAST	FIPS_OK	Generate, Reseed, Instantiate functions	On reloading the module
HMAC-SHA-1	PRF: SHA-1	KAT	CAST	FIPS_OK	HMAC tag generation	On reloading the module
HMAC-SHA2-256	PRF: SHA2-256	KAT	CAST	FIPS_OK	HMAC tag generation	On reloading the module
HMAC-SHA2-512	PRF: SHA2-512	KAT	CAST	FIPS_OK	HMAC tag generation	On reloading the module
KDF SP800-108	PRF: HMAC-SHA2-512	KAT	CAST	FIPS_OK	Counter Mode (HMAC-SHA2-512)	On reloading the module
PBKDF	Derivation of the Master Key (MK)	KAT	CAST	FIPS_OK	Key Derivation	On reloading the module

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
	PRF: HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512					
SHA-1	SHA-1	KAT	CAST	FIPS_OK	Hash	On reloading the module
SHA2-256	SHA2-256	KAT	CAST	FIPS_OK	Hash	On reloading the module
SHA2-512	SHA2-512	KAT	CAST	FIPS_OK	Hash	On reloading the module
SHA3-256	SHA3-256	KAT	CAST	FIPS_OK	Hash	On reloading the module
AES-XTS Testing Revision 2.0 (A2640)	Key_1 ≠ Key_2	CFT	Critical Function	FIPS_OK	FIPS_OK	On key generation

Table 20: Conditional Self-Tests

Each time the platform is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data has not been damaged. On Module instantiation, the Module performs the pre-operational self-tests and CASTs listed above. All KATs must complete successfully prior to any other use of cryptography by the Module.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
HMAC-SHA2-256 (A2640)	KAT	SW/FW Integrity	On Demand	Manually by reloading the module

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC	KAT	CAST	On Demand	Manually by reloading the module

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CCM	KAT	CAST	On Demand	Manually by reloading the module
AES-CMAC	KAT	CAST	On Demand	Manually by reloading the module
AES-ECB	KAT	CAST	On Demand	Manually by reloading the module
AES-GCM	KAT	CAST	On Demand	Manually by reloading the module
AES-KWP	KAT	CAST	On Demand	Manually by reloading the module
AES-GMAC	KAT	CAST	On Demand	Manually by reloading the module
AES-XTS Testing Revision 2.0	KAT	CAST	On Demand	Manually by reloading the module
Counter DRBG	KAT	CAST	On Demand	Manually by reloading the module
HMAC-SHA-1	KAT	CAST	On Demand	Manually by reloading the module
HMAC-SHA2-256	KAT	CAST	On Demand	Manually by reloading the module
HMAC-SHA2-512	KAT	CAST	On Demand	Manually by reloading the module
KDF SP800-108	KAT	CAST	On Demand	Manually by reloading the module
PBKDF	KAT	CAST	On Demand	Manually by reloading the module
SHA-1	KAT	CAST	On Demand	Manually by reloading the module
SHA2-256	KAT	CAST	On Demand	Manually by reloading the module
SHA2-512	KAT	CAST	On Demand	Manually by reloading the module

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA3-256	KAT	CAST	On Demand	Manually by reloading the module
AES-XTS Testing Revision 2.0 (A2640)	CFT	Critical Function	On key generation	On key generation

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ERROR_STATE	The error state is persistent and no services are available. Any attempt to use the Module's services result in the return of a non-zero error code.	Entered whenever one or more KAT self-tests fail or if the software integrity test fails.	The NetApp platform automatically reboots.	ERROR_STATE

Table 23: Error States

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.

10.5 Operator Initiation of Self-Tests

The operator can reload the module by rebooting the NetApp platform, fulfilling AS05.11.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module consists of a single kernel object module that provides cryptographic services as part of the NetApp ONTAP operating system. 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.

ONTAP 9.15 and greater will use the NetApp CryptoMod version 3.0 module without any required user intervention.

When used with ONTAP versions less than ONTAP 9.15, 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.

11.2 Administrator Guidance

ONTAP 9.15 and greater will use the NetApp CryptoMod version 3.0 module without any required administrator intervention.

When used with ONTAP versions less than ONTAP 9.15, 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 Non-Administrator Guidance

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
```

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.