NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Security Target

Version 1.0

14 June 2021

Prepared for:

NetApp, Inc.

1395 Crossman Ave

Sunnyvale, CA 94089

Prepared by:

leidos

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, Maryland 21046

Contents

1 Security Target Introduction 1
1.1 Security Target, Target of Evaluation, and Common Criteria Identification 1
1.2 Conformance Claims 2
1.3 Conventions 3
1.3.1 Terminology 5
1.3.2 Acronyms 7
2 TOE Description 10
2.1 TOE Overview 10
2.2 TOE Description 10
2.3 TOE Architecture 11
2.3.1 Physical Boundaries 12
2.3.2 Logical Boundaries 19
2.3.2.1 Cryptographic Support 19
2.3.2.2 User Data Protection 19
2.3.2.3 Security Management 19
2.3.2.4 Protection of the TOE Security Functionality 19
3 Documentation 19
4 Security Problem Definition 21
5 Security Objectives 22
5.1 Security Objectives for the Operational Environment 22
6 IT Security Requirements 23
6.1 Extended Requirements 23
6.2 TOE Security Functional Requirements 23
6.2.1 Cryptographic Support (FCS) 25
6.2.1.1 FCS_AFA_EXT.1 Authorization Factor Acquisition (FDE_AA) 25
6.2.1.2 FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition (FDE_AA) 25
6.2.1.3 FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys) (FDE_AA) + (FDE_EE) 25
6.2.1.4 FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key) (FDE_EE) 25
6.2.1.5 FCS_CKM.4(a)/AA Cryptographic Key Destruction (Power Management) (FDE_AA) 26
6.2.1.6 FCS_CKM.4(a)/EE Cryptographic Key Destruction (Power Management) (FDE_EE) 26
6.2.1.7 FCS_CKM.4(d) Cryptographic Key Destruction (Software TOE, 3rd Party Storage) (FDE_AA) 26
6.2.1.8 FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing) (FDE_EE) (FDE_AA) 26
6.2.1.9 FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management) (FDE_EE) (FDE_AA) 27
6.2.1.10 FCS_CKM_EXT.6 Cryptographic Key Destruction Types (FDE_EE) 27
6.2.1.11 FCS_COP.1(a) Cryptographic Operation (Signature Verification) (FDE_EE) (FDE_AA) 27
6.2.1.12 FCS_COP.1(b) Cryptographic Operation (Hash Algorithm) (FDE_EE) (FDE_AA) 27
6.2.1.13 FCS_COP.1(c) Cryptographic Operation (Keyed Hash Algorithm) (FDE_AA) 27
6.2.1.14 FCS_COP.1(d) Cryptographic Operation (Key Wrapping) (FDE_EE) (FDE_AA) 27
6.2.1.15 FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption) (FDE_EE) 28

6.2.1.16 FCS_KDF_EXT.1 Cryptographic Key Derivation (FDE_EE) (FDE_AA) 28
6.2.1.17 FCS_KYC_EXT.1 Key Chaining (Initiator) (FDE_AA) 28
6.2.1.18 FCS_KYC_EXT.2 Key Chaining (Recipient) (FDE_EE) 28
6.2.1.19 FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning (FDE_AA) 29
6.2.1.20 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) (FDE_EE) (FDE_AA) 29
6.2.1.21 FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (FDE_EE) (FDE_AA) 29
6.2.1.22 FCS_VAL_EXT.1 Validation (FDE_AA) 29
6.2.1.23 FCS_VAL_EXT.1 Validation (FDE_EE) 30
6.2.2 User Data Protection (FDP) (FDE_EE) 30
6.2.2.1 FDP_DSK_EXT.1 Protection of Data on Disk 30
6.2.3 Security Management (FMT) 30
6.2.3.1 FMT_MOF.1 Management of Functions Behavior (FDE_AA) 30
6.2.3.2 FMT_SMF.1 Specification of Management Functions (FDE_AA) 30
6.2.3.3 FMT_SMF.1 Specification of Management Functions (FDE_EE) 31
6.2.3.4 FMT_SMR.1 Security Roles (FDE_AA) 31
6.2.4 Protection of the TSF (FPT) 31
6.2.4.1 FPT_KYP_EXT.1 Protection of Key and Key Material (FDE_AA) (FDE_EE) 31
6.2.4.2 FPT_PWR_EXT.1 Power Saving States (FDE_AA) (FDE_EE) 31
6.2.4.3 FPT_PWR_EXT.2 Timing of Power Saving States (FDE_AA) (FDE_EE) 31
6.2.4.4 FPT_TST_EXT.1 TSF Testing (FDE_EE) 31
6.2.4.5 FPT_TUD_EXT.1 Trusted Update (FDE_AA) (FDE_EE) 32
6.3 TOE Security Assurance Requirements 32
6.3.1 ADV_FSP.1 Basic functional specification 33
6.3.2 AGD_OPE.1 Operational user guidance 33
6.3.3 AGD_PRE.1 Preparative procedures 34
6.3.4 ALC_CMC.1 Labelling of the TOE 34
6.3.5 ALC_CMS.1 TOE CM coverage 34
6.3.6 ATE_IND.1 Independent testing - conformance 35
6.3.7 AVA_VAN.1 Vulnerability survey 35
7 TOE Summary Specification 35
7.1 Cryptographic Support 35
7.1.1 FCS_AFA_EXT.1: Authorization Factor Acquisition (FDE_AA) 37
7.1.2 FCS_AFA_EXT.2: Timing of Authorization Factor Acquisition (FDE_AA) 37
7.1.3 FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys) (FDE_AA) (FDE_EE) 38
7.1.4 FCS_CKM.1(c): Cryptographic Key Generation (Data Encryption Key) (FDE_EE) 38
7.1.5 FCS_CKM.4(a): Cryptographic Key Destruction (Power Management) (FDE_AA) (FDE_EE). 38
7.1.6 FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage) (FDE_AA) 38
7.1.7 FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing) (FDE_EE) 44
7.1.8 FCS_CKM_EXT.4(b): Cryptographic Key and Key Material Destruction (Power Management) (FDE_EE) 44
7.1.9 FCS_CKM_EXT.6 Cryptographic Key Destruction Types (FDE_EE) 45
7.1.10 FCS_COP.1(a): Cryptographic Operation (Signature Verification) (FDE_AA) (FDE_EE) 45

7.1.11 FCS_COP.1(b): Cryptographic Operation (Hash Algorithm) (FDE_AA) (FDE_EE) 45
7.1.12 FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm) (FDE_AA) 45
7.1.13 FCS_COP.1(d): Cryptographic Operation (Key Wrapping) (FDE_AA) (FDE_EE) 45
7.1.14 FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption) (FDE_EE)..... 45
7.1.15 FCS_KDF_EXT.1: Cryptographic Key Derivation (FDE_AA) (FDE_EE) 46
7.1.16 FCS_KYC_EXT.1: Key Chaining (initiator) (FDE_AA), FCS_KYC_EXT.2 Key Chaining (Recipient) (FDE_EE) 46
7.1.17 FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning (FDE_AA) 46
7.1.18 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) (FDE_AA) (FDE_EE)46
7.1.19 FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (FDE_AA) (FDE_EE) 47
7.1.20 FCS_VAL_EXT.1/AA Validation (FDE_AA) 47
7.1.21 FCS_VAL_EXT.1/EE Validation (FDE_EE) 47
7.2 User Data Protection 47
7.2.1 FDP_DSK_EXT.1 Protection of Data on Disk (FDE_EE) 47
7.3 Security Management 48
7.3.1 FMT_MOF.1 Management of Functions Behavior (FDE_AA) 48
7.3.2 FMT_SMF.1: Specification of Management Functions (FDE_AA) 48
7.3.3 FMT_SMF.1: Specification of Management Functions (FDE_EE) 49
7.3.4 FMT_SMR.1: Security Roles (FDE_AA) 49
7.4 Protection of the TSF 49
7.4.1 FPT_KYP_EXT.1: Protection of Key and Key Material (FDE_AA) (FDE_EE) 49
7.4.2 FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States (FDE_AA) (FDE_EE) 49
7.4.3 FPT_TST_EXT.1: TSF Testing (FDE_AA) (FDE_EE) 49
7.4.4 FPT_TUD_EXT.1: Trusted Update (FDE_AA) (FDE_EE) 50
8 Protection Profile Claims 51
9 Rationale 53
9.1 TOE Summary Specification Rationale 53

List of Figures and Tables

Figure 1 Basic TOE Configuration 11
Figure 2 High-level Architecture of Authorization Acquisition and Encryption Engine 18

Table 1: Terms and Definitions 5
Table 2: Acronyms 7
Table 3 TOE Appliances 12
Table 4: Security Objectives for Operational Environment 22
Table 5: TOE Security Functional Components 23
Table 6: Assurance Components 32
Table 7: Third Party Components 32
Table 8: CryptoMod version 2.2 Algorithm Certificates 36
Table 9: NetApp Cryptographic Security Module (NCSM) Algorithm Certificates 37
Table 10 Critical Security Parameters 38
Table 11 Key Destruction 43
Table 12: HMAC Details 45
Table 13: Security Functional Requirements 51
Table 14: Security Functions vs. Requirements Mapping 53

1 Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13. It provides software-based encryption technology that ensures data at rest cannot be read if the storage medium is repurposed, returned, misplaced or stolen. The TOE supports data encryption on a volume-granular basis.

The ONTAP 9.7P13 component of the TOE is a proprietary operating system and data management software which is installed on the appliances listed below in Section 1.1 that offers unified storage for applications that read and write data over block- or file-access protocols.

The Security Target (ST) includes the following additional sections:

- TOE Description (Section 2)
- Documentation (Section 3)
- Security Problem Definition(Section 4)
- Security Objectives (Section 5)
- IT Security Requirements (Section 6)
- TOE Summary Specification (Section 7)
- Protection Profile Claims (Section 8)
- Rationale (Section 9)

1.1 Security Target, Target of Evaluation, and Common Criteria Identification

ST Title: NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 Security Target

ST Version: Version 1.0

ST Date: 14 June 2021

TOE Identification: NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13. The NVE Appliances included in the evaluated configuration are as follows:

Storage Array	Disk Type	Controller Form Factor
FAS2620	HDD/SSD	2U/12 internal drives
FAS2650	HDD/SSD	2U/24 internal drives
FAS2720	HDD/SSD	2U/12 internal drives
FAS2750	HDD/SSD	2U/24 internal drives
FAS8200 Hybrid Flash	HDD/SSD	3U
AFF A200	SSD	2U
AFF A220	NVMe Flash	2U/24 internal drives

Storage Array	Disk Type	Controller Form Factor
AFF A300	SSD	3U
AFF C190	SSD	2U/24 internal drives
AFF A800	NVMe Flash	4U/48 internal drives
AFF A320	SSD	2U
FAS9000	HDD	8U
AFF A700	SSD	8U
AFF A700s	SSD	4U/24 internal drives
FAS8300	HDD	4U
FAS8700	HDD	4U
AFF A400	SSD	4U

TOE Developer: NetApp, Inc.

Evaluation Sponsor: NetApp, Inc.

CC Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017

1.2 Conformance Claims

This ST and the TOE it describes are conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
  - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
  - Part 3 Conformant
- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata, February 1, 2019* [CPP_FDE_AA_V2.0E] with the following optional and selection-based SFRs:
  - FCS_CKM.1(b)
  - FCS_COP.1(a)
  - FCS_COP.1(b)

  - FCS_COP.1(c)
  - FCS_COP.1(d)
  - FCS_KDF_EXT.1
  - FCS_PCC_EXT.1
  - FCS_RBG_EXT.1
  - FCS_VAL_EXT.1
  - FPT_TST_EXT.1

The following NIAP Technical Decision applies to the [CPP_FDE_AA_V2.0E] and have been accounted for in the ST development and the conduct of the evaluation:

  - TD0458: FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities

- collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata, February 1, 2019 [CPP_FDE_EE_V2.0E] with the following optional and Selection-based SFRs:
  - FCS_CKM.1(b)
  - FCS_CKM.4(d)
  - FCS_COP.1(a)
  - FCS_COP.1(b)
  - FCS_COP.1(d)
  - FCS_COP.1(f)
  - FCS_KDF_EXT.1
  - FCS_RBG_EXT.1

  The following NIAP Technical Decisions apply to the [CPP_FDE_EE_V2.0E] and have been accounted for in the ST development and the conduct of the evaluation:

  - TD0458: FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities
  - TD0460: FIT Technical Decision for FPT_PWR_EXT.1 non-compliant power saving states
  - TD0464: FIT Technical Decision for FPT_PWR_EXT.1 compliant power saving states

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.

  - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by adding a string, starting with a forward slash (e.g. “FCS_CKM.1.1(b)”). Additional iterations to define which Protection Profile the SFR originated would be defined as adding a string after the first iteration (e.g. “FCS_CKM.4.1(a)/EE” or “FCS_CKM.4.1(a)/AA”).
  - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
  - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
  - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., “… **all** objects …” or “… ~~some~~ **big** things …”).
- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

1.3.1 Terminology

Table 1: Terms and Definitions

Term	Definition
Aggregates	Aggregates are containers for the disks managed by a node. An aggregate consists of one or more RAID groups.
Assurance	Grounds for confidence that a TOE meets the SFRs [CC1].
Authorization Factor	A value that a user knows, has, or is (e.g. password, token, etc.) submitted to the TOE to establish that the user is in the community authorized to use the hard disk. This value is used in the derivation or decryption of the Border Encryption Value (BEV) and eventual decryption of the DEK. Note that these values may or may not be used to establish the particular identity of the user.
Border Encryption Value (BEV)	Value passed by the FDE Authorization Acquisition (FDE-AA) component to the FDE Encryption Engine (FDE-EE) component. For FDE-AA with NVE, the BEV is the SVM-KEK associated with a given volume's VDEK.
Cluster Key Encryption Key (CKEK)	A 32-byte Key Encryption Key (KEK) that is generated via a DRBG. The CKEK is common to all nodes in the ONTAP cluster.
Cluster Passphrase	Cluster Passphrase is a 64 to 256-byte ASCII passphrase that is used as an authorization factor.
Cluster Pass-phrase Key Encryption Key (CP-KEK)	A 32-byte KEK that is derived from the cluster passphrase whose unwrapped value is derived using a passphrase based key derivation function. The CP-KEK is used to protect the CKEK.
Config Database	A persistent database containing node specific configuration data. The CDB is available to a node before the node joins a cluster.
Data Encryption Key (DEK)	A key used to encrypt data-at-rest.
FC	Fibre Channel is the original networked block protocol. Instead of files, a block protocol presents an entire virtual disk to a client. The traditional FC protocol uses a dedicated FC network with specialized FC switches and requires a client computer to also have FC network interfaces. The virtual disk is represented by a LUN, with one or more LUNs being stored in an ONTAP volume.
FCoE	FCoE is basically the same protocol as FC but uses datacenter-grade Ethernet network in place of the traditional FC transport. As with FC, the client requires an FCoE-specific network interface.
Host Platform	The local hardware and software the TOE is running on and does not include any peripheral devices (e.g. USB devices) that may be connected to the local hardware and software.
Intermediate Key	A key used in a point between the initial user authorization and the DEK.
iSCSI	iSCSI is a block protocol that can run on standard Ethernet networks. Most client operating systems offer a software initiator that runs over a standard Ethernet port.

Term	Definition
Key Chaining	The method of using multiple layers of encryption keys to protect data. A top layer key encrypts a lower layer key, which encrypts the data; this method can have any number of layers.
Key Encryption Key (KEK)	A key used to encrypt other keys, such as DEKs or storage that contains keys.
Key Material	Key material is commonly known as critical security parameter (CSP) data, and includes authorization data, nonces, and metadata.
Key Sanitization	A method of sanitizing encrypted data by securely overwriting the key that was encrypting the data.
Logical Interface	A LIF (logical interface) is an IP address or WWPN with associated characteristics, such as a role, a home port, a home node, a list of ports to fail over to, and a firewall policy. You can configure LIFs on ports over which the cluster sends and receives communications over the network.
Logical Unit Number	A LUN (logical unit number) is an identifier for a device called a logical unit addressed by a SAN protocol.
Network Attached Storage (NAS)	A NAS is a single storage device that operates on data files. A NAS unit includes a dedicated hardware device that connects to a local area network, usually through an Ethernet connection. This NAS server authenticates clients and manages file operations in much the same manner as ordinary file servers, through well-established network protocols.
NetApp CryptoMod	This module provides NIST CAVP validated cryptographic operations for NVE and the onboard key manager (OKM).
NFS	A Network File System (NFS) is the traditional file access protocol for UNIX and Linux systems. Clients can access files in ONTAP volumes using the NFSv3, NFSv4, NFSv4.1, and pNFS protocols. File access is controlled using UNIX-style permissions, NTFS-style permissions, or a combination of both.
Non-Volatile Memory	A type of computer memory that will retain information without power.
NVMe/FC	NVMe/FC, designed to work with flashed-based storage, offers scalable sessions, significantly reduced data latency, and higher throughput. NVMe/FC uses namespaces instead of LUNs. The NVMe namespaces, which are stored in an ONTAP volume, may only be accessed via the NVMe protocol.
OKM	Onboard Key Manager – Local key-management without an external KMIP server.
Operating System (OS)	Software that runs at the highest privilege level and can directly control hardware resources.
Protected Data	This refers to all data on the storage device with the exception of a small portion required for the TOE to function correctly. It is all space on the disk a user could write data to and includes the operating system, applications, and user data. Protected data does not include the Master Boot Record or Pre-authentication area of the drive – areas of the drive that are necessarily unencrypted.
RDB	ONTAP's replicated database. RDB is a quorum-based synchronous transactional data replication service used by ONTAP components to persist configuration data. The RDB is available to a node only after the node joins the cluster.
Single-node cluster	A single-node cluster is a special implementation of a cluster running on a standalone node. The TOE can deploy a single-node cluster in a branch office, for example, assuming the workloads are small enough, and that storage availability is not a critical concern.

Term	Definition
SMB/CIFS	SMB/CIFS is the traditional file access protocol for Windows systems. Clients can access files in ONTAP volumes using the SMB 2.0, SMB 2.1, SMB 3.0, and SMB 3.1.1 protocols. SMB/CIFS, like NFS, supports a mix of access permission styles.
Snapshot Copy	A Snapshot copy is a read-only, point-in-time image of a volume. It records only changes to files since the last Snapshot copy was made. A Snapshot copy can be used to recover individual files or LUNs, or to restore the entire contents of a volume.
Storage Array Networks (SAN)	A SAN is a local network of several devices. A SAN commonly uses Fibre Channel interconnects and connects a set of storage devices that share data with one another.
Submask	A submask is a bit string that can be generated and stored in a number of ways.
SVM-KEK	A 32-byte DRBG generated KEK that is associated with an individual cluster or data SVM. The SVM-KEK is used to protect DEKs used by the SVM. In FDE-AA with NVE, an SVM-KEK is a BEV.
Storage Virtual Machine	Storage virtual machines (SVMs) serve data to clients and hosts. Like a virtual machine running on a hypervisor, an SVM is a logical entity that abstracts physical resources. Data accessed through the SVM is not bound to a location in storage. Network access to the SVM is not bound to a physical port.
Target of Evaluation	A set of software, firmware, or hardware possibly accompanied by guidance. [CC1]
Volume Data Encryption Key (VDEK)	A symmetric key used to encrypt/decrypt the volume data. This may also be referred to as a Volume Encryption Key (VEK). The terms are used interchangeably in this document.
WAFL	Write Anywhere File Layout (WAFL) – The TOE's WAFL Component protects User data. The TOE uses the subject, subject's security attributes, the object, the object's security attributes and the requested operation to determine if access is granted. Like a database, WAFL uses metadata to point to actual data blocks on disk. But, unlike a database, WAFL does not overwrite existing blocks. It writes updated data to a new block and changes the metadata.
World Wide Port Name	A World Wide Port Name, (WWPN) is a World Wide Name assigned to a port in a Fibre Channel fabric. Used on storage area networks, it performs a function equivalent to the MAC address in Ethernet protocol, as it is supposed to be a unique identifier in the network.

1.3.2 Acronyms

Table 2: Acronyms

Acronym	Definition
AA	Authorization Acquisition
AES	Advanced Encryption Standard
BEV	Border Encryption Value
CBC	Cipher Block Chaining
CC	Common Criteria

Acronym	Definition
CDB	Config Database
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CPP	Collaborative Protection Profile
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
FC	Fibre Channel
FCoE	Fibre Channel over Ethernet
FDE	Full Drive Encryption
FIPS	Federal Information Processing Standards
HDD	Hard Disk Drive
HMAC	Keyed-Hash Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers
iSCSI	Internet Small Computer Systems Interface
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
IT	Information Technology
IV	Initialization Vector
KEK	Key Encryption Key
LIF	Logical Interface
LUN	Logical Unit Number
NAS	Network Attached Storage
NFS	Network File System
NIST	National Institute of Standards and Technology
NVMe/FC	Nonvolatile memory express over Fibre Channel
OS	Operating System
pNFS	Parallel NFS
PRF	Pseudo Random Function
RAID	Redundant Array of Inexpensive Disks
RBG	Random Bit Generator
RDB	ONTAP’s replicated database
RNG	Random Number Generator
RSA	Rivest Shamir Adleman Algorithm
SAN	Storage Array Networks

Acronym	Definition
SAR	Security Assurance Requirements
SED	Self-Encrypting Drive
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
SMB/CIFS	Server Message Block/ Common internet file system
SPD	Security Problem Definition
SSD	Solid State Drive
ST	Security Target
SVM	Storage Virtual Machine
SVM-KEK	Storage Virtual Machine Key Encryption Key
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
USB	Universal Serial Bus
VDEK	Volume Data Encryption Key
WAFL	Write Anywhere File Layout
wCKEK	Wrapped Cluster Key Encryption Key
wVDEK	Wrapped Volume Data Encryption Key
wSVM-KEK	Wrapped Storage Virtual Machine Key Encryption Key
WWPN	World Wide Port Name
XOR	Exclusive Or
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

2 TOE Description

2.1 TOE Overview

The TOE is the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13. The TOE provides Full Disk Encryption of HDD/SSD drives which fulfills the [CPP_FDE_EE_V2.0E] requirements. The TOE also provides the authorization acquisition to send a Border Encryption Value (BEV) to the encryption engine which fulfills the [CPP_FDE_AA_V2.0E] requirements.

2.2 TOE Description

The TOE comprises a range of disk storage appliances, consisting of storage controllers and one or more enclosures of disk storage devices (which could be HDD, SDD, or NVMe flash), running ONTAP 9.7P13. The NetApp appliances included in the TOE are listed below in Table 3.

ONTAP 9.7P13 is a proprietary operating system and data management software that provides storage for applications that read and write data over block- or file-access protocols, in storage configurations that range from high-speed flash, to lower- priced spinning media, to cloud-based object storage (not included in the evaluated configuration). All of the disk drives used in the TOE appliances are third party devices.

NetApp Volume Encryption (NVE) provides a software-based encryption technology for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen. The software-based encryption supports data encryption on a volume granular basis. Volume data is encrypted using a unique XTS-AES-256 key. Physical storage volumes are abstracted as logical entities called storage virtual machines (SVMs). In Common Criteria mode, an internal Onboard Key Manager (OKM) is used to manage the system's XTS-AES-256 keys.

A 64 to 256-byte ASCII Cluster Passphrase is used as an authorization factor. The Cluster Passphrase Key Encryption Key (CP-KEK) is derived from the Cluster Passphrase (CP) using a NIST SP 800-132 approved password-based key derivation function (PBKDFv2). Each Storage Virtual Machine (SVM) will contain a unique Storage Virtual Machine Key Encryption Key (or SVM-KEK). The SVM-KEK is a 32-byte symmetric AES key that is generated by the TOE's DRBG (CTR_DRBG) function. The SVM-KEK is protected by the CP-KEK via a NIST SP 800-38F KWP key wrapping algorithm. The protected version of an SVM-KEK is known as the wSVM-KEK. In [CPP_FDE_AA_V2.0E] with NVE, an SVM-KEK is a BEV.

NetApp Volume Encryption may be configured via the appliance's RS-232 console port. NetApp Volume Encryption also supports various networking protocols including SSH, CIFS, NFS, HTTP, HTTPs, DHCP, SNMP, Fibre Channel, and iSCSI, among others. The Protection Profile ([CPP_FDE_AA_V2.0E]) associated with this product did not consider, nor did it include, networking protocols as part of the security functional requirements and, as a result, did not include any requirements for addressing those protocols. Consequently, the protocols have not been examined as part of the required assurance activities and, therefore, no claims are made about the TOE's networking protocols.

It is suggested that a customer using the product consider the impact of using the product's SSH or HTTPs interfaces to administrate the product as opposed to the product's RS-232 console interface. The customer should base their decision on the environment in which the TOE operates and the value of the data that needs to be protected.

2.3 TOE Architecture

The TOE implementations run on NetApp-engineered FAS (Fabric Attached Storage) or AFF (All Flash FAS) appliances. Datacenter implementations of ONTAP usually deploy dedicated FAS or AFF controllers running ONTAP 9.7P13 data management software. Each controller, its storage, its network connectivity, and the instance of ONTAP running on the controller is called a node.

NetApp appliances typically are configured in cluster nodes in high-availability (HA) pairs for fault tolerance and non-disruptive operations. The Nodes communicate with each other over a private, dedicated cluster interconnect. The HA interconnect allows each node to continually check whether its partner is functioning and to mirror log data for the other's nonvolatile memory. If a node fails or if a node needs to be brought down for routine maintenance, its partner can take over its storage and continue to serve data from it. The partner gives back storage when the node is brought back on-line. The HA functionality was not covered in the scope of the evaluation or testing.

Figure 1 Basic TOE Configuration

Depending on the controller model, node storage consists of flash disks, HDDs, or both. Network ports on the controller provide access to data. Physical storage and network connectivity resources are virtualized, visible to cluster administrators only, not to NAS clients or SAN hosts.

The ONTAP 9.7P13 Data Management Software stored on the appliance, implements NIST CAVP algorithms in the NetApp CryptoMod software module to provide full disk encryption of the HDD/SSD network storage arrays. All HDD and SSD drives are provided by third party vendors. ONTAP 9.7P13 supports all the major industry standard NAS and SAN based client protocols: NFS, SMB/CIFS, FC, FCoE, iSCSI, and NVMe/FC.

The TOE encrypts data, including Snapshot copies and metadata. Volume data is encrypted using a unique XTS-AES-256 key. Each ONTAP volume is associated with one unique set of AES-XTS-256 data-encryption keys. In Common Criteria mode, an internal Onboard Key Manager (OKM) is used to manage the system's XTS-AES-256 keys.

ONTAP serves data to clients and hosts from logical containers called FlexVol volumes. FlexVol volumes contain file systems in a NAS environment and LUNs in a SAN environment. A LUN (logical unit number) is an identifier for a device called a logical unit addressed by a SAN protocol. LUNs are the basic unit of storage in a SAN configuration. A LUN represents the virtual disk stored in an ONTAP volume.

Storage virtual machines (SVMs) are similar to a virtual machine running on a hypervisor. An SVM is created by the TOE and is a logical entity that abstracts physical resources. Network access to the SVM is not bound to a physical port. An SVM serves data to clients and hosts from one or more volumes, through one or more network logical interfaces (LIFs). ONTAP volumes can be assigned to any data aggregate in the cluster. LIFs can be hosted by any physical or logical port.

The same SVM can have a LIF for NAS traffic and a separate LIF for SAN traffic. Clients and hosts need only the address of the LIF (IP address for NFS, SMB, or iSCSI; WWPN for FC) to access the SVM. LIFs keep their addresses as they move. Ports can host multiple LIFs. Each SVM has its own security, administration, and namespace.

In addition to data SVMs, ONTAP deploys special SVMs for administration:

- An admin SVM is created when the cluster is set up.
- A node SVM is created when a node joins a new or existing cluster.
- A system SVM is automatically created for cluster-level communications in an IP space.

The SVMs listed above cannot be used to serve data. There are also special LIFs for traffic within and between clusters, and for cluster and node management. All administration is performed via the CLI accessed using a console directly connected to the appliance's RS-232 port.

In addition to data volumes, ONTAP also uses the following, non-encrypted, non-client/non-data containing special volumes:

- A node root volume (typically "vol0") contains node configuration information and logs.
- An SVM root volume serves as the entry point to the namespace provided by the SVM and contains namespace directory information.
- System volumes contain special metadata such as service audit logs.

ONTAP prevents customers from storing user data on these special volumes. All user data is encrypted.

2.3.1 Physical Boundaries

The TOE is the NetApp Volume Encryption (NVE) Appliances running ONTAP 9.7P13 which provides a software-based encryption technology for third party disk drives and which is provided in the following NetApp appliances:

Table 3 TOE Appliances

Values identified are for a single HA pair specification All disk drives are third party devices.					
Storage Array	**Disk Type**	**Storage Protocols**	**Max Drives per HA Pair (HDD/SSD)**	**Controller Form Factor**	**Processor**
Intel Xeon Processor D Family					
FAS2620	HDD/SSD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	144	2U/12 internal drives	Intel Xeon D-1528 (Broadwell)

<table>
<tr><th colspan="6">Values identified are for a single HA pair specification
All disk drives are third party devices.</th></tr>
<tr><th>Storage Array</th><th>Disk Type</th><th>Storage Protocols</th><th>Max Drives per HA Pair
(HDD/SSD)</th><th>Controller Form Factor</th><th>Processor</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>2 x 64-bit 6-core 1.90 Ghz</td></tr>
<tr><td>FAS2650</td><td>HDD/SSD</td><td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB</td><td>144</td><td>2U/24 internal drives</td><td>Intel Xeon D-1528 (Broadwell)
2 x 64-bit 6-core 1.90 Ghz</td></tr>
<tr><td>FAS2720</td><td>HDD/SSD</td><td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB</td><td>144</td><td>2U/12 internal drives</td><td>Intel Xeon D-1557 (Broadwell)
2 x 64-bit 12-core 1.50 Ghz</td></tr>
<tr><td>FAS2750</td><td>HDD/SSD</td><td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB</td><td>144</td><td>2U/24 internal drives</td><td>Intel Xeon D-1557 (Broadwell)
2 x 64-bit 12-core 1.50 Ghz)</td></tr>
<tr><td>FAS8200
Hybrid Flash</td><td>HDD/SSD</td><td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB</td><td>480/480</td><td>3U</td><td>Intel Xeon D-1587 (Broadwell)
2 x 64-bit 16-core 1.70 Ghz</td></tr>
<tr><td>AFF A200</td><td>SSD</td><td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB</td><td>144</td><td>2U</td><td>Intel Xeon D-1528 (Broadwell)
2 x 64-bit 6-core 1.90 Ghz</td></tr>
<tr><td>AFF A220</td><td>NVMe Flash</td><td>FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB</td><td>144</td><td>2U/24 internal drives</td><td>Intel Xeon D-1557 (Broadwell)</td></tr>
</table>

Values identified are for a single HA pair specification

All disk drives are third party devices.

Storage Array	Disk Type	Storage Protocols	Max Drives per HA Pair (HDD/SSD)	Controller Form Factor	Processor
					2 x 64-bit 12-core 1.50 Ghz
AFF A300	SSD	NVMe/FC, FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	384	3U	Intel Xeon D-1587 (Broadwell) 2 x 64-bit 16-core 1.70 Ghz
AFF C190	SSD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	24	2U/24 internal drives	Intel Xeon D-1557 (Broadwell) 2 x 64-bit 12-core 1.50 Ghz
Intel Xeon Scalable Processors (Skylake Server)					
AFF A800	NVMe Flash	NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB	240	4U/48 internal drives	Intel Xeon Platinum 8160 (Skylake-SP) 4 x 64-bit 24-core 2.10 Ghz
AFF A320	SSD	NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB	48	2U	Intel Xeon Silver 4114 (Skylake-SP) 4 x 64-bit 10-core 2.2 Ghz
Intel Xeon Processor E5 Family					
FAS9000	HDD	FC, FCoE, iSCSI, NFS, pNFS, CIFS/SMB	1,440/480	8U	Intel Xeon E5-2697v4 (Broadwell) 4 x 64-bit 18-core 2.30 Ghz

<table>
<tr><td colspan="6">Values identified are for a single HA pair specification
All disk drives are third party devices.</td></tr>
<tr><th>Storage Array</th><th>Disk Type</th><th>Storage Protocols</th><th>Max Drives per HA Pair
(HDD/SSD)</th><th>Controller Form Factor</th><th>Processor</th></tr>
<tr><td>AFF A700</td><td>SSD</td><td>NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB</td><td>470</td><td>8U</td><td>Intel Xeon E5-2697v4 (Broadwell)
4 x 64-bit 18-core 2.30 Ghz</td></tr>
<tr><td>AFF A700s</td><td>SSD</td><td>NVMe/FC, FC, iSCSI, NFS, pNFS, CIFS/SMB</td><td>216</td><td>4U/24 internal drives</td><td>Intel Xeon E5-2697v4 (Broadwell)
4 x 64-bit 18-core 2.30 Ghz</td></tr>
<tr><td colspan="6">Cascade Lake Processor</td></tr>
<tr><td>FAS8300</td><td>HDD</td><td>FC, iSCSI, NFS, pNFS, CIFS/SMB</td><td>720</td><td>4U</td><td>Intel Xeon Silver 4210 (Cascade Lake)
4 x 64-bit 10-core 2.20 Ghz</td></tr>
<tr><td>FAS8700</td><td>HDD</td><td>FC, iSCSI, NFS, pNFS, CIFS/SMB</td><td>1440</td><td>4U</td><td>Intel Xeon Gold 5218 (Cascade Lake)
4 x 64-bit 16-core 2.3 Ghz</td></tr>
<tr><td>AFF A400</td><td>SSD</td><td>FC, iSCSI, NFS, pNFS, CIFS/SMB</td><td>480</td><td>4U</td><td>Intel Xeon Silver 4210 (Cascade Lake)
4 x 64-bit 10-core 2.20 Ghz</td></tr>
</table>

The TOE comprises storage arrays equipped with the following Intel processors:

- Broadwell microarchitecture:

  - Intel Xeon D-1528
  - Intel Xeon D-1557
  - Intel Xeon D-1587
  - Intel Xeon E5-2697 v4
- Cascade Lake microarchitecture:
  - Intel Xeon Silver 4210
  - Intel Xeon Gold 5218
- Skylake-SP microarchitecture:
  - Intel Xeon Silver 4114
  - Intel Xeon Platinum 8160.

The cryptographic modules included in the TOE have NIST Cryptographic Algorithm Validation Program (CAVP) certificates C1884 and C2114. The Operating Environments for these certificates include the following:

- Intel Xeon D-1528 (Broadwell microarchitecture), which covers the following storage arrays:
  - FAS2620, FAS2650, AFF A200: all include the Intel Xeon D-1528
  - FAS2720, FAS2750, AFF A220, AFF C190: all include the Intel Xeon D-1557, which is equivalent at the microarchitecture level to the Intel Xeon D-1528
  - FAS8200 Hybrid Flash, AFF A300: include the Intel Xeon D-1587, which is equivalent at the microarchitecture level to the Intel Xeon D-1528
  - AFF A700, AFF A700s: include the Intel Xeon E5-2697 v4, which is equivalent at the microarchitecture level to the Intel Xeon D-1528
- Intel Xeon Platinum 8160 (Skylake-SP microarchitecture), which covers the following storage arrays:
  - AFF A800: includes the Intel Xeon Platinum 8160
  - AFF A320: includes the Intel Xeon Silver 4114, which is equivalent at the microarchitecture level to the Intel Xeon Platinum 8160
- Intel Xeon Silver 4210 (Cascade Lake microarchitecture), which covers the following storage arrays:
  - FAS8300, AFF A400: include the Intel Xeon Silver 4210
  - FAS8700: includes the Intel Xeon Gold 5218, which is equivalent at the microarchitecture level to the Intel Xeon Silver 4210.

Therefore, all storage arrays included in the evaluated configuration are covered by the C2114 and C1884 certificates, because they either include the same processor on which the certified algorithm testing was performed, or they include a processor that is equivalent at the microarchitecture level to a processor on which algorithm testing was performed.

A High-level Architecture of Authorization Acquisition and Encryption Engine is provided below.

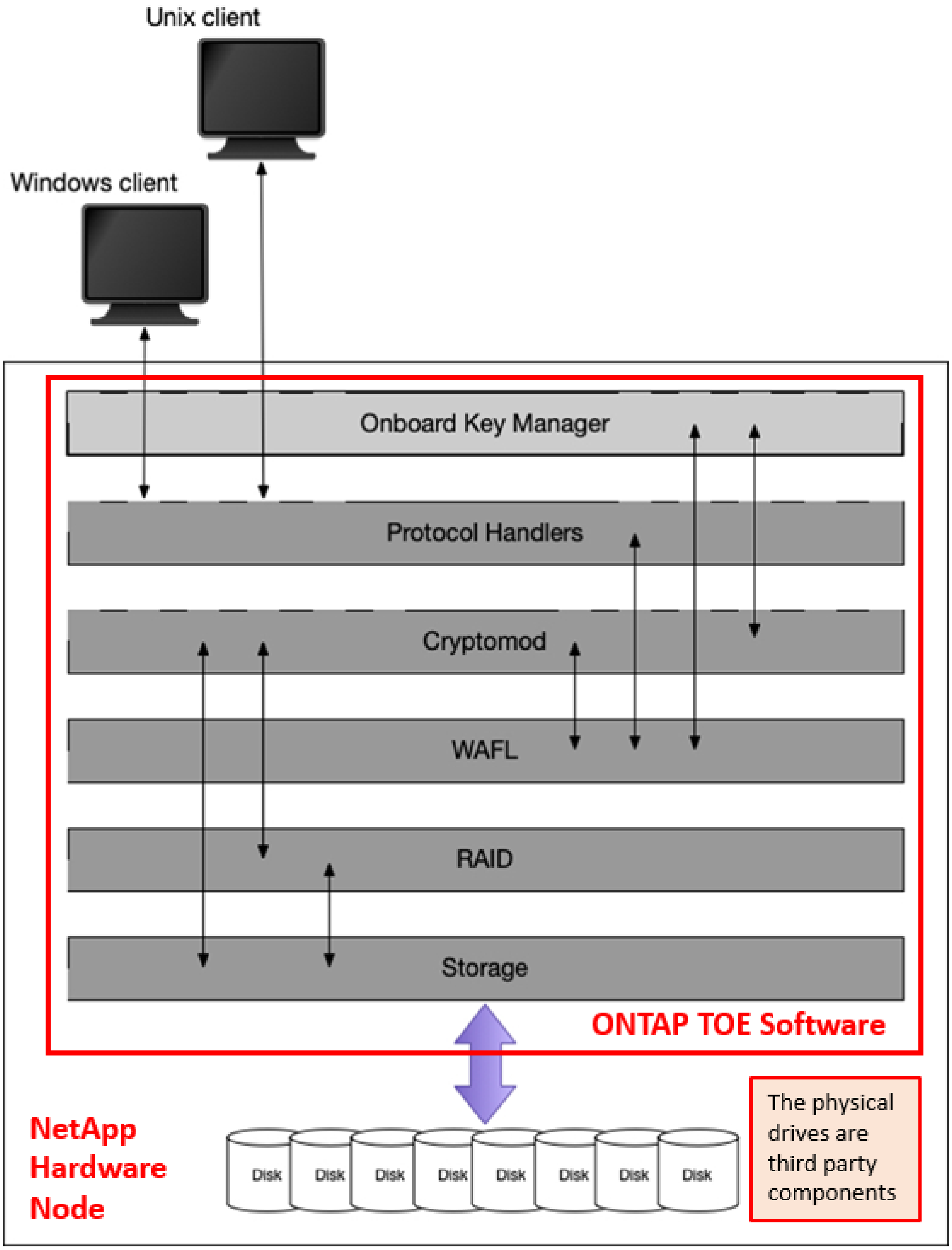

Figure 2 High-level Architecture of Authorization Acquisition and Encryption Engine

The simplified figure above includes the following components:

1. External clients sending NFS (UNIX) and/or SMB/CIFS (Windows) data that interact with a protocol handler.
2. The Onboard Key Manager which is used to:
    a. Provide a customer facing CLI;
    b. Service ONTAP client key generation requests;
    c. Request the cluster passphrase at boot.
3. CryptoMod, a NIST CAVP validated kernel module providing
    a. A DRBG (CTR_DRBG) for symmetric key generation and salts;
    b. XTS-AES encryption/decryption routines;
    c. Key encryption/decryption routines;
    d. SHA-2 digest functions;
    e. Non-persistent key-storage kept within non-volatile memory.
4. WAFL, ONTAP's "write anywhere" file system layer, that:
    a. Optimizes client reads/writes via compression and deduplication;
    b. Provides IO buffers to RAID;
    c. Provides persistent storage for the wVDEK.
    d. Writes the key ID associated with the volume to an on-disk data structure when an encrypted volume is first created,
    e. Decides what is (and is not) encrypted;
    f. Passes the appropriate key ID, along with data indicating if the associated buffers need to be encrypted (decrypted), to RAID to write (read) to (from) the disk.
5. RAID, the component responsible for
    a. Encrypting/decrypting the WAFL IO buffers;
    b. Calculating/comparing both plaintext and ciphertext checksums on IO buffers;
    c. Providing protection against drive failures.
6. Storage, an ONTAP component that writes (reads) the IO to (from) the drives.
7. The physical drives are third party components.

2.3.2 Logical Boundaries

This section identifies the logical boundaries provided by the ONTAP 9.7P13 Data Management Software and the NetApp appliances:

- Cryptographic Support
- User Data Protection
- Security Management
- Protection of the TSF

2.3.2.1 Cryptographic Support

The TOE includes NIST CAVP-validated cryptographic algorithms supporting cryptographic functions. The TOE provides Key Wrapping, Key Derivation, BEV Validation, and data encryption.

2.3.2.2 User Data Protection

The TOE performs Full Drive Encryption such that the drive contains no plaintext user data. The TOE performs user data encryption by default in the out-of-the-box configuration using XTS-AES-256 mode.

2.3.2.3 Security Management

The TOE supports management functions for changing and erasing the DEK and initiating the TOE firmware updates using a command line interface.

2.3.2.4 Protection of the TOE Security Functionality

The TOE provides trusted firmware updates, protects Key and Key Material; and supports power saving states. The TOE runs a suite of self-tests during initial start-up (on power on).

3 Documentation

The following documents, part of the ONTAP 9.7P13 documentation set, are included in the TOE documentation:

- Commands: Manual Page Reference, November 2019
- NetApp Encryption Power Guide, May 2021
- System Administration Reference, April 2020
- Upgrade Express Guide, January 2020
- Upgrade and Revert/Downgrade Guide, April 2020.

These documents, as well as all others in the documentation set, are available via the following URLs:

- http://docs.netapp.com/ontap-9/index.jsp

- https://docs.netapp.com/us-en/ontap/
- https://www.netapp.com/us/documentation/ontap-and-oncommand-system-manager.aspx

4 Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) from the [CPP_FDE_AA_V2.0E] and the [CPP_FDE_EE_V2.0E].

In general, the [CPP_FDE_AA_V2.0E] and [CPP_FDE_EE_V2.0E] have presented a Security Problem Definition appropriate for requirements for Data-at-Rest protection for a lost device that contains storage, and as such is applicable to the NetApp Storage Systems running ONTAP 9.7P13 TOE.

5 Security Objectives

The [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] have presented a Security Objectives statement appropriate for Data-at-Rest protection, and as such is applicable to the NetApp Storage Systems running ONTAP 9.7P13 TOE.

5.1 Security Objectives for the Operational Environment

Table 4: Security Objectives for Operational Environment

Objective	Description
OE.TRUSTED_CHANNEL	Communication among and between product components (i.e., AA and EE) is sufficiently protected to prevent information disclosure.
OE.INITIAL_DRIVE_STATE	The OE provides a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption.
OE.PASSPHRASE_STRENGTH	An authorized administrator will be responsible for ensuring that the passphrase authorization factor conforms to guidance from the Enterprise using the TOE.
OE.POWER_DOWN	Volatile memory is cleared after power-off so memory remnant attacks are infeasible.
OE.SINGLE_USE_ET	External tokens that contain authorization factors will be used for no other purpose than to store the external token authorization factor.
OE.STRONG_ENVIRONMENT_CRYPTO	The Operating Environment will provide a cryptographic function capability that is commensurate with the requirements and capabilities of the TOE and Appendix A.
OE.TRAINED_USERS	Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors.
OE.PLATFORM_STATE	The platform in which the storage device resides (or an external storage device is connected) is free of malware that could interfere with the correct operation of the product.
OE.PLATFORM_I&A	The Operational Environment will provide individual user identification and authentication mechanisms that operate independently of the authorization factors used by the TOE.
OE.PHYSICAL	The Operational Environment will provide a secure physical computing space such than an adversary is not able to make modifications to the environment or to the TOE itself.

6 IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the TOE and to scope the evaluation effort.

The SFRs have all been drawn from the [CPP_FDE_AA_V2.0E] and the [CPP_FDE_EE_V2.0E].

As a result, any selection, assignment, or refinement operations already performed by that Protection Profile (PP) on the claimed SFRs are not identified here (i.e., they are not formatted in accordance with the conventions specified in section 1.3 of this ST). Formatting conventions are only applied on SFR text that was chosen at the ST author's discretion.

6.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [CPP_FDE_AA_V2.0E] and the [CPP_FDE_EE_V2.0E]. This ST references the following extended SFRs.

- FCS_AFA_EXT.1 Authorization Factor Acquisition
- FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition
- FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)
- FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)
- FCS_CKM_EXT.6 Cryptographic Key Destruction Types
- FCS_KDF_EXT.1 Cryptographic Key Derivation
- FCS_KYC_EXT.1 Key Chaining (Initiator)
- FCS_KYC_EXT.2 Key Chaining (Recipient)
- FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning
- FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)
- FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
- FCS_VAL_EXT.1 Validation
- FDP_DSK_EXT.1 Protection of Data on Disk
- FPT_KYP_EXT.1 Protection of Key and Key Material
- FPT_PWR_EXT.1 Power Saving States
- FPT_PWR_EXT.2 Timing of Power Saving States
- FPT_TST_EXT.1 TSF Testing
- FPT_TUD_EXT.1 Trusted Update

6.2 TOE Security Functional Requirements

Table 5 identifies the SFRs satisfied by the TOE.

Table 5: TOE Security Functional Components

Requirement Class	Requirement Component
FCS: Cryptographic Support	FCS_AFA_EXT.1: Authorization Factor Acquisition
	FCS_AFA_EXT.2: Timing of Authorization Factor Acquisition

Requirement Class	Requirement Component
	FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)
	FCS_CKM.1(c): Cryptographic Key Generation (Data Encryption Key)
	FCS_CKM.4(a)/AA: Cryptographic Key Destruction (Power Management)
	FCS_CKM.4(a)/EE: Cryptographic Key Destruction (Power Management)
	FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage)
	FCS_CKM_EXT.4(a): Cryptographic Key and Key Material Destruction (Destruction Timing)
	FCS_CKM_EXT.6: Cryptographic Key Destruction Types
	FCS_COP.1(a): Cryptographic Operation (Signature Verification)
	FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)
	FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm)
	FCS_COP.1(d): Cryptographic Operation (Key Wrapping)
	FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_KDF_EXT.1: Cryptographic Key Derivation
	FCS_KYC_EXT.1: Key Chaining (Initiator)
	FCS_KYC_EXT.2: Key Chaining (Recipient)
	FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning
	FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)
	FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
	FCS_VAL_EXT.1: Validation
FDP: User Data Protection	FDP_DSK_EXT.1: Protection of Data on Disk
FMT: Security Management	FMT_MOF.1: Management of Functions Behavior
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TSF	FPT_KYP_EXT.1: Protection of Key and Key Material
	FPT_PWR_EXT.1: Power Saving States

Requirement Class	Requirement Component
	FPT_PWR_EXT.2: Timing of Power Saving States
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Trusted Update

6.2.1 Cryptographic Support (FCS)

6.2.1.1 FCS_AFA_EXT.1 Authorization Factor Acquisition (FDE_AA)

FCS_AFA_EXT.1.1 The TSF shall accept the following authorization factors: [

- ***a submask derived from a password authorization factor conditioned as defined in FCS_PCC_EXT.1***

].

6.2.1.2 FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition (FDE_AA)

FCS_AFA_EXT.2.1 The TSF shall reacquire the authorization factor(s) specified in FCS_AFA_EXT.1 upon transition from any Compliant power saving state specified in FPT_PWR_EXT.1 prior to permitting access to plaintext data.

6.2.1.3 FCS_CKM.1(b) Cryptographic Key Generation (Symmetric Keys) (FDE_AA) + (FDE_EE)

FCS_CKM.1.1(b) The TSF shall generate symmetric cryptographic keys using a Random Bit Generator as specified in FCS_RBG_EXT.1 and specified cryptographic key sizes [***256 bit***] that meet the following: [no standard].

Application Note: The TOE implements the Cluster Key Encryption Key (CKEK) and the Storage Virtual Machine Key Encryption Key (SVM-KEK) as symmetric keys used along the key chain. The TOE protects the CKEK by using the AES-256 key CP-KEK to wrap the CKEK. The TOE protects the SVM-KEK by using the AES-256 key CKEK to wrap the SVM-KEK.

6.2.1.4 FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key) (FDE_EE)

FCS_CKM.1.1(c) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation method [

- ***generate a DEK using the RBG as specified in FCS_RBG_EXT.1***

and specified cryptographic key sizes [***256 bits***].

Application Note: The TOE generates AES-256 KEKs (NIST-KWP algorithm) and AES-XTS-256 keys using the NetApp CryptoMod CTR_DRBG. The XTS-AES specification describes two keys as being used: an AES encryption/decryption key and a "tweak" key. In this document, the phrase "XTS-AES" key refers to both keys as a single entity.

6.2.1.5 FCS_CKM.4(a)/AA Cryptographic Key Destruction (Power Management) (FDE_AA)

FCS_CKM.4.1(a)/AA The TSF shall [***erase***] cryptographic keys and key material from volatile memory when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1 that meets the following: [a key destruction method specified in FCS_CKM.4(d)].

6.2.1.6 FCS_CKM.4(a)/EE Cryptographic Key Destruction (Power Management) (FDE_EE)

FCS_CKM.4.1(a)/EE The TSF shall [***erase***] cryptographic keys and key material from volatile memory when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1 that meets the following: [a key destruction method specified in FCS_CKM_EXT.6].

6.2.1.7 FCS_CKM.4(d) Cryptographic Key Destruction (Software TOE, 3rd Party Storage) (FDE_AA)

FCS_CKM.4.1(d) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

- ***For volatile memory, the destruction shall be executed by a [***
  - ***single overwrite consisting of [***
    - ***a pseudo-random pattern using the TSF's RBG,***
    - ***zeroes,***
  - ***removal of power to the memory];***
- ***For non-volatile storage that consists of the invocation of an interface provided by the underlying platform that [***
  - ***logically addresses the storage location of the key and performs a [single] overwrite consisting of [***
    - ***a pseudo-random pattern using the TSF's RBG,***
    - ***zeroes]***

]

that meets the following: [no standard].

6.2.1.8 FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing) (FDE_EE) (FDE_AA)

FCS_CKM_EXT.4.1(a) The TSF shall destroy all keys and key material when no longer needed.

6.2.1.9 FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management) (FDE_EE) (FDE_AA)

FCS_CKM_EXT.4.1(b) The TSF shall destroy all key material, BEV, and authentication factors stored in plaintext when transitioning to a Compliant power saving state as defined by FPT_PWR_EXT.1.

6.2.1.10 FCS_CKM_EXT.6 Cryptographic Key Destruction Types (FDE_EE)

FCS_CKM_EXT.6.1 The TSF shall use [***FCS_CKM.4(d)***] key destruction methods.

6.2.1.11 FCS_COP.1(a) Cryptographic Operation (Signature Verification) (FDE_EE) (FDE_AA)

FCS_COP.1.1(a) The TSF shall perform [cryptographic signature services (verification)] in accordance with a [

- ***RSA Digital Signature Algorithm with a key size (modulus) of [3072-bit***]

that meet the following: [

- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes***

].

6.2.1.12 FCS_COP.1(b) Cryptographic Operation (Hash Algorithm) (FDE_EE) (FDE_AA)

FCS_COP.1.1(b) The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [***SHA-256, SHA-384, SHA-512***] that meet the following: [**ISO/IEC 10118-3:2004**].

6.2.1.13 FCS_COP.1(c) Cryptographic Operation (Keyed Hash Algorithm) (FDE_AA)

FCS_COP.1.1(c) The TSF shall perform cryptographic [keyed-hash message authentication] in accordance with a specified cryptographic algorithm [***HMAC-SHA-512***] and cryptographic key sizes [**L1 = 2,048, L2 = 512**] that meet the following: [**ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"**].

6.2.1.14 FCS_COP.1(d) Cryptographic Operation (Key Wrapping) (FDE_EE) (FDE_AA)

FCS_COP.1.1(d) The TSF shall perform [key wrapping] in accordance with a specified cryptographic algorithm [AES] in the following modes **[*KWP*]** and the cryptographic key size [***256 bits***] that meet the following: [AES as specified in ISO/IEC 18033-3, ***[NIST SP 800-38F]***].

6.2.1.15 FCS_COP.1(f) Cryptographic Operation (AES Data Encryption/Decryption) (FDE_EE)

FCS_COP.1.1(f) The TSF shall perform [data encryption and decryption] in accordance with a specified cryptographic algorithm [AES used in ***[XTS]*** mode] and cryptographic key sizes [***256 bits***] that meet the following: [AES as specified in ISO/IEC 18033-3, ***[XTS as specified in IEEE 1619]***].

6.2.1.16 FCS_KDF_EXT.1 Cryptographic Key Derivation (FDE_EE) (FDE_AA)

FCS_KDF_EXT.1.1 The TSF shall accept [***a conditioned password submask***] to derive an intermediate key, as defined in [

- ***NIST SP 800-132***]

using the keyed-hash functions specified in FCS_COP.1(c), such that the output is at least of equivalent security strength (in number of bits) to the BEV.

6.2.1.17 FCS_KYC_EXT.1 Key Chaining (Initiator) (FDE_AA)

FCS_KYC_EXT.1.1 The TSF shall maintain a key chain of: [

- ***intermediate keys originating from one or more submask(s) to the BEV using the following method(s): [***
  - ***key derivation as specified in FCS_KDF_EXT.1,***
  - ***key wrapping as specified in FCS_COP.1(d),***

while maintaining an effective strength of [***256 bits***] for symmetric keys and an effective strength of [***not applicable***] for asymmetric keys.

FCS_KYC_EXT.1.2 The TSF shall provide at least a [***256 bit***] BEV to [**encryption engine**] [

- ***after the TSF has successfully performed the validation process as specified in FCS_VAL_EXT.1***].

6.2.1.18 FCS_KYC_EXT.2 Key Chaining (Recipient) (FDE_EE)

FCS_KYC_EXT.2.1 The TSF shall accept a BEV of at least [***256 bits***] from [**the AA**].

FCS_KYC_EXT.2.2 The TSF shall maintain a chain of intermediary keys originating from the BEV to the DEK using the following method(s): [

key wrapping as specified in FCS_COP.1(d)]
while maintaining an effective strength of [***256 bits***] for symmetric keys and an effective strength of [***not applicable***] for asymmetric keys.

6.2.1.19 FCS_PCC_EXT.1 Cryptographic Password Construct and Conditioning (FDE_AA)

FCS_PCC_EXT.1.1 A password used by the TSF to generate a password authorization factor shall enable up to [**256**] characters in the set of {upper case characters, lower case characters, numbers, and [**all printable ASCII characters**]} and shall perform Password-based Key Derivation Functions in accordance with a specified cryptographic algorithm HMAC-[***SHA-512***], with [**1024**] iterations, and output cryptographic key sizes [***256 bits***] that meet the following: [NIST SP 800-132].

6.2.1.20 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) (FDE_EE) (FDE_AA)

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with [***[NIST SP 800-90A]***] using [***CTR_DRBG (AES)***].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [

- ***[2] software-based noise source(s),***
- ***[2] hardware-based noise source(s)***]

with a minimum of [***256 bits***] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

6.2.1.21 FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (FDE_EE) (FDE_AA)

FCS_SNI_EXT.1.1 The TSF shall [***use salts that are generated by a [DRBG as specified in FCS_RBG_EXT.1]***].

FCS_SNI_EXT.1.2 The TSF shall use [***no nonces***].

FCS_SNI_EXT.1.3 The TSF shall create IVs in the following manner [

- ***XTS: No IV. Tweak values shall be non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer***].

6.2.1.22 FCS_VAL_EXT.1 Validation (FDE_AA)

FCS_VAL_EXT.1.1/AA The TSF shall perform validation of the [***submask***] using the following method(s): [

- ***key wrap as specified in FCS_COP.1(d)***].

FCS_VAL_EXT.1.2/AA The TSF shall require validation of the [BEV] prior to [forwarding the BEV to the EE].

FCS_VAL_EXT.1.3/AA The TSF shall [

- ***require power cycle/reset the TOE after [1] of consecutive failed validation attempts***].

Application Note: If an incorrect cluster passphrase is entered at boot, then ONTAP will attempt to boot, but the storage component will not be able to authenticate to the NSE drives. Consequently, ONTAP will not see any drives and will panic, resulting in a system reboot.

While attempting to recover from a failure in the boot media, if an incorrect cluster passphrase is entered at boot, then ONTAP will attempt to boot, but the storage component will not be able to authenticate to the NSE drives. Consequently, ONTAP will not see any drives and will panic, resulting in a system reboot.

6.2.1.23 FCS_VAL_EXT.1 Validation (FDE_EE)

FCS_VAL_EXT.1.1/EE The TSF shall perform validation of the [***BEV***] using the following method(s): [

- ***key wrap as specified in FCS_COP.1(d)]***

FCS_VAL_EXT.1.2/EE The TSF shall require validation of the [***BEV***] prior to [**allowing access to TSF data after exiting a Compliant power saving state**].

FCS_VAL_EXT.1.3/EE The TSF shall [

- ***require power cycle/reset the TOE after [1] of consecutive failed validation attempts***].

6.2.2 User Data Protection (FDP) (FDE_EE)

6.2.2.1 FDP_DSK_EXT.1 Protection of Data on Disk

FDP_DSK_EXT.1.1 The TSF shall perform Full Drive Encryption in accordance with FCS_COP.1(f), such that the drive contains no plaintext protected data.

FDP_DSK_EXT.1.2 The TSF shall encrypt all protected data without user intervention.

6.2.3 Security Management (FMT)

6.2.3.1 FMT_MOF.1 Management of Functions Behavior (FDE_AA)

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behaviour of] the functions [use of Compliant power saving state] to [authorized users].

6.2.3.2 FMT_SMF.1 Specification of Management Functions (FDE_AA)

FMT_SMF.1.1/AA The TSF shall be capable of performing the following management functions: [

a) forwarding requests to change the DEK to the EE,
b) forwarding requests to cryptographically erase the DEK to the EE,
c) allowing authorized users to change authorization factors or set of authorization factors used,

d) initiate TOE firmware/software updates,

e) ***[no other functions]]***].

6.2.3.3 FMT_SMF.1 Specification of Management Functions (FDE_EE)

FMT_SMF.1.1/EE The TSF shall be capable of performing the following management functions: [

a) change the DEK, as specified in FCS_CKM.1, when re-provisioning or when commanded,

b) erase the DEK, as specified in FCS_CKM.4(a),

c) initiate TOE firmware/software updates,

d) ***[no other functions]***].

6.2.3.4 FMT_SMR.1 Security Roles (FDE_AA)

FMT_SMR.1.1 The TSF shall maintain the roles [authorized user].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.4 Protection of the TSF (FPT)

6.2.4.1 FPT_KYP_EXT.1 Protection of Key and Key Material (FDE_AA) (FDE_EE)

FPT_KYP_EXT.1.1 The TSF shall [

- ***only store keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d), or encrypted, as specified in FCS_COP.1(g) or FCS_COP.1(e)].***

6.2.4.2 FPT_PWR_EXT.1 Power Saving States (FDE_AA) (FDE_EE)

FPT_PWR_EXT.1.1[1] The TSF shall define the following Compliant power saving states: [***G3, G2(S5)***].

6.2.4.3 FPT_PWR_EXT.2 Timing of Power Saving States (FDE_AA) (FDE_EE)

FPT_PWR_EXT.2.1 For each Compliant power saving state defined in FPT_PWR_EXT.1.1, the TSF shall enter the Compliant power saving state when the following conditions occur: user-initiated request, [***shutdown***].

6.2.4.4 FPT_TST_EXT.1 TSF Testing (FDE_EE)

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [***during initial start-up (on power on), at the conditions [before the function is first invoked]***] to demonstrate the correct operation of the TSF: [**cryptographic algorithm tests, software integrity test**].

[1] Modified per TD0464

6.2.4.5 FPT_TUD_EXT.1 Trusted Update (FDE_AA) (FDE_EE)

FPT_TUD_EXT.1.1 The TSF shall provide [authorized users] the ability to query the current version of the TOE [***software***].

FPT_TUD_EXT.1.2 The TSF shall provide [authorized users] the ability to initiate updates to TOE [***software***].

FPT_TUD_EXT.1.3 The TSF shall verify updates to the TOE software using a [***digital signature as specified in FCS_COP.1(a)***] by the manufacturer prior to installing those updates.

6.3 TOE Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 1 augmented with the *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata, February 1, 2019 and the *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata, February 1, 2019. The assurance components are summarized in the following table:

Table 6: Assurance Components

Requirement Class	Requirement Component
ADV: Development	Basic Functional Specification (ADV_FSP.1)
AGD: Guidance Documents	Operational User Guidance (AGD_OPE.1)
	Preparative Procedures (AGD_PRE.1)
ALC: Life Cycle Support	Labeling of the TOE (ALC_CMC.1)
	TOE CM Coverage (ALC_CMS.1)
ATE: Tests	Independent Testing – Sample (ATE_IND.1)
AVA: Vulnerability Assessment	Vulnerability Survey (AVA_VAN.1)

Requirement

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR**,** including a proprietary Key Management Description (Appendix E), and **[Entropy Essay, list of all of 3rd party software libraries (including version numbers), 3rd party hardware components (including model/version numbers)].**

Table 7: Third Party Components

Component	Model/ Version Number
Third Party Hardware Components	
Solid State Drive (SSD)	FAS 2650: X440_PHM2800MCTO A800: X4010S172B1T9NTE FAS 8300: X440_PHM2800MCTO, X440_TPM3V800AMD

Hard Disk Drive	FAS 9000: X440_PHM2800MCTO)
Third Party Software Components	
OpenSSL	OpenSSL 1.0.2s-fips
Intel ISA-L Crypto Library	v2.22 Intel Intelligent Storage Acceleration Library Crypto

6.3.1 ADV_FSP.1 Basic functional specification

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

6.3.2 AGD_OPE.1 Operational user guidance

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

AGD_OPE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.3 AGD_PRE.1 Preparative procedures

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

6.3.4 ALC_CMC.1 Labelling of the TOE

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

ALC_CMC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.5 ALC_CMS.1 TOE CM coverage

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.
ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.3.6 ATE_IND.1 Independent testing - conformance

ATE_IND.1.1D	The developer shall provide the TOE for testing.
ATE_IND.1.1C	The TOE shall be suitable for testing.
ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.3.7 AVA_VAN.1 Vulnerability survey

AVA_VAN.1.1D	The developer shall provide the TOE for testing.
AVA_VAN.1.1C	The TOE shall be suitable for testing.
AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

7 TOE Summary Specification

This Section describes the following security functions:

- Cryptographic Support
- User Data Protection
- Security Management
- Protection of the TSF

7.1 Cryptographic Support

All TOE cryptographic services are provided by the NetApp software modules CryptoMod version 2.2 and the NetApp Cryptographic Security Module (NCSM). NetApp's CryptoMod module is used to:

- Generate salts and keying material via a validate DRBG.
- Derive keys via PBKDFv2.
- Calculate cryptographic hashes.
- Encrypt/decrypt data using validated AES encryption/decryption modes.
- Calculate HMACs.
- Encrypt keys using KWP-AE.
- Decrypt keys using KWP-AD.
- Store volatile keys.
- Zeroize volatile keys.

The NetApp Cryptographic Security Module is used to validate the TOE's cryptographically signed images using approved cryptographic hash and digital signature validation algorithms. All cryptographic algorithms are NIST CAVP certified. The following tables identify the cryptographic algorithms used by the TSF, the associated standards to which they conform, and the NIST certificates that demonstrate that the claimed conformance has been met.

Table 8: CryptoMod version 2.2 Algorithm Certificates

SFR	Algorithm	Standard	Certificate
Cryptographic Operation (Hash Algorithm)			
FCS_COP.1.1(b)	SHA-256, SHA-512	ISO/IEC 10118-3:2004	C1884: SHA2-256 C1884: SHA2-512
Cryptographic Operation (Keyed Hash Algorithm)			
FCS_COP.1.1(c)	HMAC-512	ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”	C1884: HMAC-SHA2-512
Cryptographic Operation (Key Wrapping)			
FCS_COP.1.1(d)	AES-KWP-256	NIST SP 800-38F	C1884: AES-KWP
Cryptographic Operation (AES Data Encryption/Decryption)			
FCS_COP.1.1(f)	AES-XTS-256	XTS as specified in [IEEE 1619].	C1884: AES-XTS
Cryptographic Operation (Random Bit Generation)			
FCS_RBG_EXT.1	AES-256 (CTR_DRBG)	NIST SP 800-90A	C1884: Counter DRBG

Table 9: NetApp Cryptographic Security Module (NCSM) Algorithm Certificates

SFR	Algorithm	Standard	Certificate
Cryptographic Operation (Signature Verification)			
FCS_COP.1.1(a)	RSA 3072	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes	C2114: RSA SigVer (FIPS186-4)
Cryptographic Operation (Hash Algorithm)			
FCS_COP.1.1(b)	SHA-256 SHA-384 SHA-512	ISO/IEC 10118-3:2004	C2114: SHA2-256 C2114: SHA2-384 C2114: SHA2-512

7.1.1 FCS_AFA_EXT.1: Authorization Factor Acquisition (FDE_AA)

The cluster passphrase serves as the password authorization factor. The cluster passphrase serves as the password authorization factor. In CC mode, the cluster passphrase (64-256 bytes) must be entered at boot before ONTAP is allowed to boot. The Cluster Passphrase Key Encryption Key (CP-KEK) is derived from the Cluster Passphrase (CP) and the Cluster Salt using a NIST SP 800-132 approved password-based key derivation function (PBKDFv2).

There are three operations that require a user to enter the existing cluster passphrase:

1. Whenever the cluster passphrase is changed (security key-manager onboard update-passphrase).
2. When booting ONTAP (CC mode only).
3. When recovering from a failure in the boot media.

7.1.2 FCS_AFA_EXT.2: Timing of Authorization Factor Acquisition (FDE_AA)

The TOE provides the Compliant power saving states of G3 (mechanical off) and G2(S5) (soft off).

An authorized user can execute the `system halt` command which causes the system to enter the G2(S5) state. The `system halt` command is not needed if the TOE is powered off by a mechanical switch or by “pulling the plug”.

The Compliant power saving states require the cluster passphrase be entered at boot before ONTAP is allowed to boot.

7.1.3 FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys) (FDE_AA) (FDE_EE)

The TOE generates 256 bit keys using the TOE's DRBG to create the Cluster Key Encryption Key (CKEK) and the Storage Virtual Machine Key Encryption Key (SVM-KEK) as symmetric keys used along the key chain. The TOE protects the CKEK by using the AES-256 key CP-KEK to wrap the CKEK. The TOE protects the SVM-KEK by using the AES-256 key CKEK to wrap the SVM-KEK.

7.1.4 FCS_CKM.1(c): Cryptographic Key Generation (Data Encryption Key) (FDE_EE)

The TOE generates AES-XTS-256 keys using the NetApp CryptoMod CTR_DRBG. The XTS-AES specification describes two keys as being used: an AES encryption/decryption key and a "tweak" key. In this document, the phrase "XTS-AES" key refers to both keys as a single entity. Therefore, the XTS-AES operations that use AES-256 will utilize a 512-bit XTS-AES "key".

The keys are stored in the NetApp CryptoMod Key Table.

7.1.5 FCS_CKM.4(a): Cryptographic Key Destruction (Power Management) (FDE_AA) (FDE_EE)

The TOE provides the Compliant power saving states of G3 (mechanical off) and G2(S5) (soft off).

An authorized user can execute the `system halt` command which causes the system to enter the G2(S5) state. The `system halt` command is not needed if the TOE is powered off by a mechanical switch or by "pulling the plug" where all key values in volatile memory drain to a zero state.

The keys not persistently stored are stored in CryptoMod's volatile memory.

7.1.6 FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage) (FDE_AA)

The following table identifies the Critical Security Parameters (CSPs) used by the TOE. The table identifies the usage of each CSP, the type, the source of origination, and where each is stored in memory.

Table 10 Critical Security Parameters

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
CP	Authorization factor	64 to 256-byte ASCII passphrase	Supplied by cluster administrator when "security key-manager setup" is	Temporarily "stored" as a variable/register in functions involved in the	Not stored in non-volatile memory.	1,2

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
			executed, when "security key-manager onboard update-passphrase" is executed and when ONTAP is rebooted.	calculation of the CP-KEK. Not stored in the CryptoMod key table.		
CP-Salt	Salt used with CP when creating CP Hash	64-byte random salt	CryptoMod DRBG	Temporarily "stored" as a variable/register in functions involved in the calculation of the CP-KEK or functions that need to store the CP-Salt in non-volatile memory. Not stored in the CryptoMod key table.	Persistently stored in non-volatile memory in an RDB table and the OKM database.	2,3
CP-Hash	Used to validate the CP	SHA-256(CP-Salt || CP)	CryptoMod SHA-256 performed on the CP	Temporarily "stored" as a variable/register in functions that need to validate the cluster passphrase, or functions that need to store the CP-Hash in non-volatile memory. Not stored in the CryptoMod key table.	Persistently stored in non-volatile memory within an RDB table.	2,3

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
Cluster-Salt	Salt used in creation of CP-KEK	64-byte random salt	CryptoMod DRBG	Temporarily "stored" as a variable/register in functions that need to calculate the CP-KEK, or functions that need to store the Cluster-Salt in non-volatile memory. Not stored in the CryptoMod key table.	Persistently stored in non-volatile memory within an RDB table and the OKM DB.	2,3,4
CP-KEK	Used to protect the CKEK.	AES-256 key derived using PBKDF2 function with HMAC-SHA-512 used as the PRF (1024 iterations).	CryptoMod PBKDF2	Temporarily "stored" as a variable/register in functions that need to wrap/unwrap the CKEK. Stored in CryptoMod's key table.	Not stored in non-volatile memory.	2,5
CKEK	Used to protect each of the SVM-KEKs.	AES-256 key	CryptoMod DRBG	Temporarily "stored" as a variable/register in functions that need to wrap/unwrap keys wrapped by the CKEK. Stored in CryptoMod's key table.	Not stored in non-volatile memory.	2,5
wCKEK	Encrypted form of CKEK	Wrapped (encrypted) form of CKEK using [NIST 800-38F]	CryptoMod KWP	Temporarily "stored" as a variable/register in functions that	Persistently stored in non-volatile memory within an RDB	2,3,4

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
		KWP-AE with CP-KEK used as the encrypting key		need to calculate the wCKEK, functions that need to unwrap the wCKEK, or functions that need to store the wCKEK in non-volatile memory. Not stored in the CryptoMod key table.	table and the OKM DB.	
SVM-KEK	Used to protect VDEKs associated with the SVM's volumes	AES-256 key	CryptoMod DRBG	Temporarily "stored" as a variable/register in functions that need to calculate the wSVM-KEK or functions that need to use the SV-KEK to unwrap a key that was wrapped by the SVM-KEK. Stored in CryptoMod's key table.	Not stored in non-volatile memory.	2,5
wSVM-KEK	Encrypted form of SVM-KEK. The wSVM-KEK is identified as the BEV in NVE systems.	Wrapped (encrypted) form of SVM-KEK using [NIST 800-38F] KWP-AE with CKEK used as the encrypting key	CryptoMod KWP	Temporarily "stored" as a variable/register in functions that need to access the wSVM-KEK, functions that need to unwrap the wSVM-KEK, or functions that need to	Persistently stored in RDB table's non-volatile memory and CDB table's non-volatile memory.	2,3,6

Name	Use	Type	Source	Storage within Volatile Memory	Storage within non-volatile Memory	Notes
				store the wSVM-KEK in non-volatile memory. Not stored in the CryptoMod key table.		
VDEK	Used to encrypt data associated with a volume	XTS-AES-256 generated key.	CryptoMod DRBG	Temporarily "stored" as a variable/register in functions that need to use the VDEK as an encryption key. Stored in CryptoMod's key table.	Not stored in non-volatile memory.	5,7,8
wVDEK	Encrypted form of a VDEK	Wrapped (encrypted) form of a VDEK using [NIST 800-38F] KWP-AE with the corresponding SVM-KEK used as the encrypting key	CryptoMod KWP	Temporarily "stored" as a variable/register in functions that need to wrap the VDEK, functions that need to unwrap the wVDEK, or functions that need to store the wVDEK in non-volatile memory. Is not stored in CryptoMod's key table.	Persistently stored with WAFL on-disk (i.e. non-volatile) data structures.	6,7,8

Notes:

1. The cluster passphrase (CP) is required when setting up OKM, when updating the passphrase, when ONTAP reboots, and when performing a recovery operation.
2. Key belongs to the NVE FDE-AA component.

3. RDB is the replicated, cluster-wide database used by ONTAP.
4. The OKM DB file, located at */cfcard/kmip/km_onboard.wkeydb*, contains the cluster salt, the node salt (not used in Common Criteria mode), encrypted key material (wCKEK), encrypted key material (wNSE-AK1, wNSE-AK2) not used for NVE, and key IDs. When the Onboard Key Manager is deleted, the contents of the OKM DB are zeroized.
5. The CryptoMod key table memory utilizes memory that is auto zeroed during core dumps.
6. The CDB is a node-specific configuration database available prior to a node joining a cluster.
7. The XTS-AES "key" is best thought of as two independent AES-256 bit keys (key1 and key2) that are stored as a single 512-bit entity.
8. Key belongs to the NVE FDE-EE component.

The TOE temporarily stores key material such as the unwrapped DEK and the PBKDFv2 based upon the cluster passphrase, CP-Salt, and Cluster salt. The TOE clears the keys from memory by removal of power. The TOE also clears the keys when they are no longer needed.

The NetApp CryptoMod `crypto_secure_zero()` function is used for clearing volatile memory. The TOE will overwrite the key material with random bytes from the DRBG, then overwrite the location with zeroes, and then perform a read verify of the zeroes.

The `SecureFileDeleter::remove()` function is used for clearing non-volatile storage. The TOE will overwrite the file with random data, overwrite the file with zeroes, read verify the file contains only zeroes, and then delete the file.

The "volume delete" command takes an optional parameter "-force". When the "volume delete" command is used with the "-force true" parameter, then the volume is not moved to the recovery-queue; therefore, the VDEK keys associated with the volume are deleted immediately. If the "-force true" command is not used, then the keys associated with the volume are deleted only when the volume is automatically deleted from the recovery-query or when the volume is purged from the recovery-queue. ONTAP's default behavior is to delete volumes from the recovery-queue after they have been in the queue for 24-hours.

The following table describes the circumstances under which each of the keys are destroyed or deleted.

Table 11 Key Destruction

Key	Destroyed when	Deleted when
CP-KEK	OKM deleted. (Note 1, 2)	System powered off or rebooted.
CKEK	OKM deleted. (Note 1)	System powered off or rebooted.
wCKEK	OKM deleted. (Note 1)	N/A

Key	Destroyed when	Deleted when
SVM-KEK	OKM deleted. (Note 1) Vserver deleted (Note 3)	System powered off or rebooted.
wSVM-KEK	OKM deleted. (Note 1) Vserver deleted (Note 2)	N/A
VDEK	OKM deleted. (Note 1) Volume deleted.	System powered off or rebooted.
wVDEK	OKM deleted. (Note 1) Volume deleted.	N/A

Notes:

1. OKM cannot be deleted if any encrypted volumes exist within the ONTAP cluster.
2. When the cluster passphrase is changed, the old CP-KEK is destroyed.
3. An SVM cannot be deleted if the SVM contains encrypted volumes.

7.1.7 FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing) (FDE_EE)

The TOE shall delete all keys and key material when the storage volume they are protecting has been deleted. The VDEKs are automatically deleted when the corresponding volume is deleted. The key hierarchy itself is deleted when all volumes are deleted, and the following command is run: `security key-manager onboard disable`.

The CP-KEK is destroyed when the Onboard Key Manager is deleted, with the CP-KEK being zeroized in the CryptoMod key table.

7.1.8 FCS_CKM_EXT.4(b): Cryptographic Key and Key Material Destruction (Power Management) (FDE_EE)

The TOE provides the Compliant power saving states of G3 (mechanical off) and G2(S5) (soft off).

An authorized user can execute the `system halt` command which causes the system to enter the G2(S5) state. The system halt command is not needed if the TOE is powered off by a mechanical switch or by "pulling the plug" where all key values in volatile memory drain to a zero state.

The CP-KEK; CKEK; SVM-KEK; VDEK keys are stored temporarily as a variable/register in CryptoMod's key table. Table 10 identifies the keys stored in volatile memory.

The keys stored in volatile memory can also be cleared by the removal of power, where the memory locations drain to zero. Any key stored in a DIMM (main system memory) is deleted when entering the G3 or G2(S5) states. Unwrapped keys are only stored in DIMMs.

7.1.9 FCS_CKM_EXT.6 Cryptographic Key Destruction Types (FDE_EE)

The TOE clears its keys in accordance with FCS_CKM.4(d).

7.1.10 FCS_COP.1(a): Cryptographic Operation (Signature Verification) (FDE_AA) (FDE_EE)

The TOE implements the RSA Digital Signature Algorithm with a key size (modulus) of 3072-bit with SHA-384 signatures to verify authenticity of the trusted updates. Upon receiving an update and the signature file, the TOE uses the embedded public key stored in the firmware on the NetApp Appliance. The TOE will verify the signature before installing it and reject any update with an invalid signature.

7.1.11 FCS_COP.1(b): Cryptographic Operation (Hash Algorithm) (FDE_AA) (FDE_EE)

The TOE performs SHA-256, SHA-384, and SHA-512 cryptographic hashing services that meet the following: ISO/IEC 10118-3:2004. SHA-256 is used in generating the CP-Hash value used in validating the CP when it is entered by an administrator. The TOE uses the SHA-384 hash functions as part of the RSA signature verification function for the trusted updates. The TOE uses the SHA-512 has function as part of the PBKDFv2 to produce the cluster passphrase and in support of the HMAC-SHA-512.

7.1.12 FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm) (FDE_AA)

The TOE performs HMAC-SHA-512 message authentication using cryptographic key sizes L2 = 512, L1 = 2048 bits that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.

The PBKDFv2 function uses HMAC-SHA512 (the CP-SALT is used as the key) with 1024 rounds.

Table 12: HMAC Details

HMAC Function	Key Length	Block Size	Output MAC Length	Hash Function Used
HMAC-SHA-512	L2 = 512, L1 = 2048	1024	512	SHA-512

7.1.13 FCS_COP.1(d): Cryptographic Operation (Key Wrapping) (FDE_AA) (FDE_EE)

The TOE uses the NIST 800-38F KWP-AE(P) routine to encrypt (or "wrap") a key and the corresponding NIST 800-38F KWP-AD(C) routine to decrypt ("unwrap") an encrypted, or wrapped, key.

7.1.14 FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption) (FDE_EE)

The TOE performs data encryption and decryption using a unique XTS-AES-256 key, as the data is written to or read from the disks.

7.1.15 FCS_KDF_EXT.1: Cryptographic Key Derivation (FDE_AA) (FDE_EE)

The TOE implements PBKDFv2 with HMAC-SHA-512, 1024 iterations, and a salt value of 512 bits to transform the cluster passphrase into a derived intermediate key that provides the base of the key chain resulting in the BEV as specified in SP800-132. The output is at least of equivalent security strength (in number of bits) to the BEV.

7.1.16 FCS_KYC_EXT.1: Key Chaining (initiator) (FDE_AA), FCS_KYC_EXT.2 Key Chaining (Recipient) (FDE_EE)

The TOE uses the PBKDFv2 key derivation function to transform the cluster passphrase into 256-bit BEV; in which it uses AES-KWP to unwrap the DEKs and store them in the NetApp CryptoMod key table. The AES-KWP unwrap function will verify the correctness of the cluster passphrase. Once verified, the TOE will have access to the DEK values.

7.1.17 FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning (FDE_AA)

The TOE accepts passwords up to 256 characters. The character set can consist of all upper-case characters, lower case characters, numbers, and all printable ASCII characters. The password is conditioned using PBDKFv2 that meets SP800-132. The cryptographic algorithm implements HMAC-SHA-512, a salt value of 512 bits from the DRBG, and 1024 iterations to produce a cryptographic key size of 256-bits.

7.1.18 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) (FDE_AA) (FDE_EE)

Random bits are produced by a DRBG implemented within the NetApp CryptoMod module. The DRBG uses the CTR_DRBG algorithm from NIST SP 800-90A. 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. Entropy will be provided from OS's /dev/random device, which can provide up to 512 bits of entropy.

The CTR_DRBG (AES) is seeded with at least 384-bits from:

- 2 software-based noise sources
  - Software interrupts
  - Event driven interrupts
- 2 hardware-based noise sources
  - Ethernet interrupts
  - Intel RDRAND instruction set (when supported by the CPU)

7.1.19 FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) (FDE_AA) (FDE_EE)

The TOE generates salts using its CTR_DRBG (AES). The XTS-AES algorithm does not use initialization vectors or nonces. Tweak values are non-negative integers, assigned consecutively, and starting at an arbitrary non-negative integer, with a length of 256-bits (32 bytes).

7.1.20 FCS_VAL_EXT.1/AA Validation (FDE_AA)

The Cluster Passphrase is a 64–256-byte customer generated ASCII string that is used as an authorization factor. The Cluster Passphrase is used in conjunction with a salt value to derive a cluster passphrase key encryption key (CP-KEK) via a NIST SP 800-132 ([NIST 800-132]) approved PBKDFv2 algorithm. The CP-Hash is used by OKM when there is a need to validate that the CP has been entered correctly by a storage administrator.

During booting ONTAP or recovering from a failure in the boot media, if an incorrect cluster passphrase is entered at boot, then ONTAP will boot, but the WAFL component will not be able to mount any user data volumes. As a consequence, ONTAP will not be able to service any user data. This condition can only be cleared by rebooting the node and entering the correct passphrase.

When modifying the cluster passphrase, a customer is allowed 5 consecutive failed attempts to authenticate with the current cluster passphrase. After 5 consecutive failed attempts, the cluster passphrase may be modified only by (a) rebooting one or more nodes within the cluster, or (b) waiting for 24 hours to elapse before re-attempting to modify the cluster passphrase.

7.1.21 FCS_VAL_EXT.1/EE Validation (FDE_EE)

The cluster passphrase authorization factor is used to support validation. The key wrap in FCS_COP.1(d) is used, the validation is performed inherently.

The cluster passphrase has to be entered at boot when the TOE is configured for CC Mode. Once ONTAP boots, if the cluster passphrase is incorrect, no unwrapped keys are available for use (i.e. all encrypted volumes will remain offline). The only way to recover is to manually reboot and enter the correct passphrase.

7.2 User Data Protection

7.2.1 FDP_DSK_EXT.1 Protection of Data on Disk (FDE_EE)

The TOE ensures that it encrypts all the storage devices entirely when a user or administrator first provisions the TOE. Configuring OKM in CC mode constitutes “first time provisioning”.

The encryption of any protected data does not depend on a user electing to protect that data. The drive encryption occurs transparently to the user and the decision to protect the data is outside the discretion of the user. The RAID layer encrypts (decrypts) 4k block of user data using AES-XTS-256 when writing to (reading from) the drives.

Provided that the write-path buffer received by RAID from WAFL needs to be encrypted, the RAID component:

- Passes the data, along with the VEK key ID (which RAID gets from WAFL) to the NetApp CryptoMod;
- Calculates a checksum over the unencrypted and encrypted data;
- Writes the encrypted data (and encrypted checksum) to disk;
- Sets an on-disk flag indicating that the checksum is calculated over the encrypted data.

On the read path, RAID:

- Reads the data along with the checksum;
- Determines if the stored checksum was performed over encrypted or unencrypted data;
- Checks that the stored checksum and a checksum over the data agree;
- Decrypts the data if the stored checksum was performed over encrypted data;
- Returns the (decrypted) data to WAFL.

Only Data Volumes are encrypted. Data on a root volume, an SVM root volume is not encrypted.

WAFL encrypts all user data, there is metadata (not available to a user) that is not encrypted.

The following persistent data is not encrypted:

- The root aggregate, which does not contain any user data, is not encrypted.
- The boot media (example: compact flash), which does not contain user data, is not encrypted.
- Fingerprint data (used for deduplication) is not encrypted.

7.3 Security Management

7.3.1 FMT_MOF.1 Management of Functions Behavior (FDE_AA)

The TOE provides the Compliant power saving states of G3 (mechanical off) and G2(S5) (soft off).

The TOE enters the G3 (mechanical off) state when the administrator removes the device power via a mechanical switch. The TOE must be fully rebooted from this state.

An authorized user can execute the `system halt` command which causes the system to enter the G2(S5) state. The TOE must be fully rebooted from this state.

7.3.2 FMT_SMF.1: Specification of Management Functions (FDE_AA)

The TOE supports the management functions:

- The TOE forwards requests to change the DEK to the EE. The authorized user executes a `volume encryption rekey` command to change the DEK, as specified in FCS_CKM.1.
- The TOE cryptographically erases the DEK via the authorized user execution of the `volume delete` command.
- The TOE permits authorized users to change authorization factors or set of authorization factors used by the `security key-manager onboard update-passphrase` command.

- The TOE initiates TOE firmware/software updates via `cluster image update` command.

7.3.3 FMT_SMF.1: Specification of Management Functions (FDE_EE)

The TOE supports the management functions:

- The TOE changes the DEK, as specified in FCS_CKM.1 via a `volume encryption rekey` command.
- The TOE cryptographically erases the DEK via by `volume delete` command as specified in FCS_CKM.4(a).
- The TOE initiates TOE firmware/software updates via `cluster image update` command.

7.3.4 FMT_SMR.1: Security Roles (FDE_AA)

The TOE maintains the role of authorized user.

7.4 Protection of the TSF

7.4.1 FPT_KYP_EXT.1: Protection of Key and Key Material (FDE_AA) (FDE_EE)

The TOE stores keys in non-volatile memory when wrapped, as specified in FCS_COP.1(d). The NetApp CryptoMod module uses the NIST 800-38F KWP-AE(P) routine to encrypt (or "wrap") a key and the corresponding NIST 800-38F KWP-AD(C) routine to decrypt ("unwrap") an encrypted, or wrapped, key. Routines utilize the NetApp CryptoMod AES routines to perform the encryption/decryption.

The ONTAP Onboard Key Manager (OKM) uses the OKM database (file location: */cfcard/kmip/km_onboard.wkeydb*) and ONTAP's replicated database (RDB) whenever it has a need to persistently store the wrapped keys in non-volatile memory. ONTAP's RDB is a quorum-based synchronous transactional data replication service used by ONTAP components to persist configuration data.

7.4.2 FPT_PWR_EXT.1: Power Saving States / FPT_PWR_EXT.2: Timing of Power Saving States (FDE_AA) (FDE_EE)

The TOE provides the Compliant power saving states of G3 (mechanical off) and G2(S5) (soft off).

The TOE enters the G3 (mechanical off) state when the administrator removes the device power via a mechanical switch. The TOE must be fully rebooted from this state.

An authorized user can execute the `system halt` command which causes the system to enter the G2(S5) state. The TOE must be fully rebooted from this state.

7.4.3 FPT_TST_EXT.1: TSF Testing (FDE_AA) (FDE_EE)

The TOE includes power-on self-tests to ensure that the TOE is operating correctly. The power-on self-tests include a Known Answer Test (KAT) to verify the correctness of the cryptographic algorithms and the software integrity test to ensure that the module is not corrupted.

The KATs for cryptographic functions consist of executing each function on data for which the correct answer is already known. The output produced by the tested function is compared with the known answer. If they are not identical, the KAT fails.

The TOE includes the following power-on self-tests to ensure that the cryptographic functionality is performing correctly:

The Known Answer Tests (KATs) include the following:

- AES-128 CBC, AES-256 CBC – encryption/decryption test
- DRBG – Tested per SP800-90A, including the Health Testing identified in Section 11.3.
- HMAC SHA-512 - keyed-hash message authentication code test
- PBKDF2 - Password-Based Key Derivation Function 2 test
- SHA-256, SHA-384, SHA-512 - hashing test
- XTS-AES-128, XTS-AES-256 – AES encryption/decryption
- RSA Signature Generation/Verification – 2048 bits and 3072-bits

The TOE performs the following software integrity test to ensure that the module is not corrupted.

- Software integrity test - During power-on self-testing, the module performs a self-integrity check and compares the results against the build time generated hash digests. During power on, the bootloader validates the whitelist database of secure boot keys with the signature associated with each module that is loaded. After each module is validated and loaded, the boot process continues with the ONTAP initialization. If signature validation fails for any module, the system reboots.

7.4.4 FPT_TUD_EXT.1: Trusted Update (FDE_AA) (FDE_EE)

The TSF provides authorized users the ability to query the current version of the TOE. The administrator executes the `cluster image show` or the `version` command to display the current version of the TOE.

NetApp code signing ensures that ONTAP images installed through non-disruptive image updates or automated non-disruptive image updates are authentically produced by NetApp and have not been tampered with. The NetApp updates are cryptographically signed using a RSA Digital Signature algorithm with a key size of 3072-bits with a SHA-384 signature. The private keys, used for code signing, are stored in a limited access HSM at NetApp. If the TOE’s public keys are tampered with then an update will fail.

The TOE will verify the signature before installing the update and reject any update with an invalid signature.

This is a no-touch security feature for upgrading ONTAP versions. The user is not expected to do anything differently except for optionally verifying the top-level image.tgz signature.

8 Protection Profile Claims

The ST conforms to:

- *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition*, Version 2.0 + Errata, February 1, 2019 [cPP_FDE_AA_V2.0E] with the following optional and selection-based SFRs: FCS_CKM.1(b), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(c), FCS_COP.1(d), FCS_KDF_EXT.1, FCS_PCC_EXT.1, FCS_RBG_EXT.1, FCS_VAL_EXT.1, FPT_TST_EXT.1.
- *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata, February 1, 2019 [cPP_FDE_EE_V2.0E] with the following optional and Selection-based SFRs: FCS_CKM.1(b), FCS_CKM.4(b), FCS_CKM.4(d), FCS_COP.1(a), FCS_COP.1(b), FCS_COP.1(d), FCS_COP.1(f), FCS_KDF_EXT.1, FCS_RBG_EXT.1.

As explained in Section 3, the Security Problem Definition of the [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] have been included by reference into this ST.

As explained in Section 5, Security Objectives, the Security Objectives of the [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] have been included by reference into this ST.

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is reproduced from the [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] and operations completed as appropriate.

Table 13: Security Functional Requirements

Requirement Class	Requirement Component	Source
FCS: Cryptographic Support	FCS_AFA_EXT.1 Authorization Factor Acquisition	[cPP_FDE_AA_V2.0E]
	FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition	[cPP_FDE_AA_V2.0E]
	FCS_CKM.1(b): Cryptographic Key Generation (Symmetric Keys)	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FCS_CKM.1(c) Cryptographic Key Generation (Data Encryption Key)	[cPP_FDE_EE_V2.0E]
	FCS_CKM.4(a)/AA: Cryptographic Key Destruction (Power Management)	[cPP_FDE_AA_V2.0E]
	FCS_CKM.4(a)/EE: Cryptographic Key Destruction (Power Management)	[cPP_FDE_EE_V2.0E]
	FCS_CKM.4(d): Cryptographic Key Destruction (Software TOE, 3rd Party Storage)	[cPP_FDE_AA_V2.0E]
	FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing)	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]

Requirement Class	Requirement Component	Source
	FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management)	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FCS_CKM_EXT.6 Cryptographic Key Destruction Types	[cPP_FDE_EE_V2.0E]
	FCS_COP.1(a): Cryptographic Operation (Signature Verification)	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FCS_COP.1(b): Cryptographic Operation (Hash Algorithm)	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FCS_COP.1(c): Cryptographic Operation (Keyed Hash Algorithm)	[cPP_FDE_AA_V2.0E]
	FCS_COP.1(d): Cryptographic Operation (Key Wrapping)	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FCS_COP.1(f): Cryptographic Operation (AES Data Encryption/Decryption)	[cPP_FDE_EE_V2.0E]
	FCS_KDF_EXT.1: Cryptographic Key Derivation	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FCS_KYC_EXT.1: Key Chaining (Initiator)	[cPP_FDE_AA_V2.0E]
	FCS_KYC_EXT.2: Key Chaining (Recipient)	[cPP_FDE_EE_V2.0E]
	FCS_PCC_EXT.1: Cryptographic Password Construct and Conditioning	[cPP_FDE_AA_V2.0E]
	FCS_RBG_EXT.1: Cryptographic Operation (Random Bit Generation)	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FCS_SNI_EXT.1: Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FCS_VAL_EXT.1: Validation	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
FDP: User Data Protection	FDP_DSK_EXT.1: Protection of Data on Disk	[cPP_FDE_EE_V2.0E]
FMT: Security Management	FMT_MOF.1: Management of Functions Behavior	[cPP_FDE_AA_V2.0E]
	FMT_SMF.1: Specification of Management Functions	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FMT_SMR.1: Security Roles	[cPP_FDE_AA_V2.0E]
FPT: Protection of the TSF	FPT_KYP_EXT.1: Protection of Key and Key Material	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]

Requirement Class	Requirement Component	Source
	FPT_PWR_EXT.1: Power Saving States	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FPT_PWR_EXT.2: Timing of Power Saving States	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FPT_TST_EXT.1: TSF Testing	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]
	FPT_TUD_EXT.1: Trusted Update	[cPP_FDE_AA_V2.0E] [cPP_FDE_EE_V2.0E]

9 Rationale

This security target includes by reference the [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the [cPP_FDE_AA_V2.0E] / [cPP_FDE_EE_V2.0E] assumptions. [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] application notes and assurance activities. Consequently, [cPP_FDE_AA_V2.0E] and [cPP_FDE_EE_V2.0E] rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

9.1 TOE Summary Specification Rationale

Each subsection in Section 7, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The security functions work together to satisfy all of the security functional requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 7, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. Table 7 Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

Table 14: Security Functions vs. Requirements Mapping

Specification	Cryptographic support	User Data Protection	Security management	Protection of the TSF
FCS_AFA_EXT.1	X			
FCS_AFA_EXT.2	X			
FCS_CKM.1(b)	X			

Specification	Cryptographic support	User Data Protection	Security management	Protection of the TSF
FCS_CKM.1(c)	X			
FCS_CKM.4 (a)	X			
FCS_CKM.4 (c)	X			
FCS_CKM.4 (d)	X			
FCS_CKM.4 (e)	X			
FCS_CKM_EXT.4 (a)	X			
FCS_CKM_EXT.4 (b)	X			
FCS_CKM_EXT.6	X			
FCS_COP.1(a)	X			
FCS_COP.1(b)	X			
FCS_COP.1(c)	X			
FCS_COP.1(d)	X			
FCS_COP.1(f)	X			
FCS_KDF_EXT.1	X			
FCS_KYC_EXT.1	X			
FCS_KYC_EXT.2	X			
FCS_PCC_EXT.1	X			
FCS_RBG_EXT.1	X			
FCS_SNI_EXT.1	X			
FCS_VAL_EXT.1	X			
FDP_DSK_EXT.1		X		
FMT_MOF.1			X	
FMT_SMF.1			X	
FMT_SMR.1			X	
FPT_KYP_EXT.1				X
FPT_PWR_EXT.1				X
FPT_PWR_EXT.2				X
FPT_TUD_EXT.1				X
FPT_TST_EXT.1				X