RackTop Systems

RackTop SHIELD v1.0

v1.2

Security Target



Document Version: 1.2

Prepared for:

RACKTOP

Prepared by:

Corsec

RackTop Systems
13454 Sunrise Valley Drive
Suite 550
Herndon, VA 20171
United States of America
Phone: +1 443 276 6973
www.racktopsystems.com

Corsec Security, Inc.
12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America
Phone: +1 703 267 6050
www.corsec.com

Table of Contents

1. Introduction 6
1.1 Purpose 6
1.2 Security Target and TOE References 6
1.3 Product Overview 7
1.4 TOE Overview 7
1.5 TOE Environment 7
1.6 TOE Description 7
1.6.1 Physical Scope 7
1.6.2 TOE Delivery 9
1.6.3 Logical Scope 9
1.6.4 Product Physical/Logical Features and Functionality not included in the TOE 10
2. Conformance Claims 11
3. Security Problem Definition 12
3.1 Threats 12
3.1.1 T.UNAUTHORIZED _DATA_ACCESS 12
3.1.2 T.KEYING_MATERIAL_COMPROMISE 12
3.1.3 T.AUTHORIZATION_GUESSING 12
3.1.4 T.KEYSPACE_EXHAUST 12
3.1.5 T.UNAUTHORIZED_UPDATE 13
3.2 Assumptions 13
3.2.1 A.INITIAL_DRIVE_STATE 13
3.2.2 A.SECURE_STATE 13
3.2.3 A.TRUSTED_CHANNEL 13
3.2.4 A.TRAINED_USER 13
3.2.5 A.PLATFORM_STATE 14
3.2.6 A.SINGLE_USE_ET 14
3.2.7 A.POWER_DOWN 14
3.2.8 A.PASSWORD_STRENGTH 14
3.2.9 A.PLATFORM_I&A 14
3.2.10 A.STRONG_CRYPTO 14
3.2.11 A.PHYSICAL 14
3.3 Organizational Security Policy 15
4. Security Objectives 16
4.1 Security Objectives for the Operational Environment 16
4.1.1 OE.TRUSTED_CHANNEL 16
4.1.2 OE.INITIAL_DRIVE_STATE 16
4.1.3 OE.PASSPHRASE_STRENGTH 16
4.1.4 OE.POWER_DOWN 16
4.1.5 OE.SINGLE_USE_ET 16
4.1.6 OE.STRONG_ENVIRONMENT_CRYPTO 16
4.1.7 OE.TRAINED_USERS 16
4.1.8 OE.PLATFORM_STATE 17
4.1.9 OE.PLATFORM_I&A 17
4.1.10 OE.PHYSICAL 17
5. Extended Components 18

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6. Security Assurance Requirements 19
7. Security Functional Requirements 20
7.1 Conventions 20
7.2 Security Functional Requirements 20
7.2.1 Class FCS: Cryptographic Support 21
FCS_CKM_EXT.4(a) Cryptographic Key and Key Material Destruction (Destruction Timing) 21
FCS_CKM_EXT.4(b) Cryptographic Key and Key Material Destruction (Power Management) 21
FCS_COP.1(a) Cryptographic Operation (Signature Verification) 22
FCS_COP.1(b) Cryptographic Operation (Hash Algorithm) 22
FCS_KYC_EXT.1 Key Chaining (Initiator) 22
FCS_SNI_EXT.1 Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation) 22
7.2.2 FMT_MOF.1 Management of Functions Behavior 23
FMT_SMF.1 Specification of Management Functions 23
FMT_SMR.1 Security Roles 23
7.2.3 Protection of the TSF (FPT) 23
FPT_KYP_EXT.1 Protection of Key and Key Material 23
FPT_PWR_EXT.1 Power Saving States 23
FPT_PWR_EXT.2 Timing of Power Saving States 23
FPT_TUD_EXT.1 Trusted Update 24
8. TOE Summary Specification 25
8.1 TOE Security Functionality 25
8.1.1 Cryptographic Support 25
8.1.2 Security Management 28
8.1.3 Protection of the TSF 29
9. Rationale 30
9.1 Conformance Claims Rationale 30
9.1.1 Variance Between the PP and this ST 30
9.1.2 Security Assurance Requirements Rationale 30
9.1.3 Dependency Rationale 30
10. Acronyms and Terms 31
10.1 Acronyms 31

List of Figures

Figure 1 – TOE Boundary 8

List of Tables

Table 1 – ST and TOE References 6
Table 2 – Guidance Documentation 9
Table 3 – CC and PP Conformance 11
Table 4 – NIAP FDE AA Technical Decisions 11

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table 5 – Security Assurance Requirements 19
Table 6 – TOE Security Functional Requirements 20
Table 7 – Mapping of TOE Security Functionality to Security Functional Requirements 25
Table 8 - CAVP Algorithm Certificate References 25
Table 9– Files required for validation of the software package 27
Table 10 – Acronyms 31

 ©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2025-08-11	Dayanandini Pathmanathan	Initial draft - addressed customer comments and submission to lab.
0.2	2025-09-23	Dayanandini Pathmanathan	Addressing lab comments.
0.3	2026-01-05	Dayanandini Pathmanathan	Addressing lab comments.
0.4	2026-01-21	Dayanandini Pathmanathan	Addressing lab comments.
0.5	2026-03-09	Dayanandini Pathmanathan	Addressing lab comments.
0.6	2026-03-24	Kathleen Moyer	Updates to algorithms.
0.7	2026-04-07	Dayanandini Pathmanathan	Adding CAVP certificates.
0.8	2026-05-20	Dayanandini Pathmanathan	Internal reviews and submission to Lab.
0.9	2026-08-05	Dayanandini Pathmanathan	Minor updates based on lab comments.
1.0	2026-08-12	Dayanandini Pathmanathan	Minor updates based on lab comments.
1.1	2026-09-18	Dayanandini Pathmanathan	Addressing ACA comments.
1.2	2026-10-06	Dayanandini Pathmanathan	Minor updates to TOE Boundary diagram.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the RackTop SHIELD v1.0 and will hereafter be referred to as the TOE throughout this document.

1.1 Purpose

This ST is divided into ten sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, Organizational Security Policies (OSPs), and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in Part 2 or CC Part 3.
- Security Assurance Requirements (Section 6) – Presents the SARs met by the TOE.
- Security Functional Requirements (Section 7) – Presents the SFRs met by the TOE.
- TOE Summary Specification (Section 8) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 9) – Presents the rationale for the SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 10) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	RackTop Systems RackTop SHIELD v1.0 Security Target
ST Version	Version 1.2
ST Author	Corsec Security, Inc.
ST Publication Date	October 6, 2026
TOE Reference	RackTop SHIELD v1.0

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.3 Product Overview

RackTop Encrypted Boot (RackTop SHIELD v1.0) is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

1.4 TOE Overview

The TOE is RackTop SHIELD v1.0, an authorization acquisition product that obtains and manages authorization data used to access encrypted data stored on TCG-compliant SEDs utilizing FIPS 140-2 or 140-3 validated cryptographic modules.

The TOE provides authorization acquisition and drive unlock functionality as part of a two-layer encryption strategy in accordance with CSfC Data-at-Rest (DAR) Capability Package guidance, specifically fulfilling the Outer Layer Encryption role. It ensures that storage media remains inaccessible unless proper authorization data is presented in the form of 256-bit keys protected by physical separation from the host system.

1.5 TOE Environment

- The TOE operates on platforms that use Trusted Computing Group (TCG) Opal 2.0 (or equivalent) SEDs.
- Encryption and decryption of user data is performed entirely by the hardware encryption engine inside the SED.
- The TOE assumes the underlying SEDs correctly enforce encryption policies and secure key handling as per their FIPS validation.
- Userspace is provided by a modern Linux operating system which provides strong crypto and exposes a FIPS compliant DRBG implementation via OpenSSL.

It is assumed that there will be no untrusted users or software on the TOE Server components. In addition, the TOE is intended to be deployed in a physically secured cabinet, room, or data center with the appropriate level of physical access control and physical protection (e.g. badge access, fire control, locks, alarms, etc.).

1.6 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

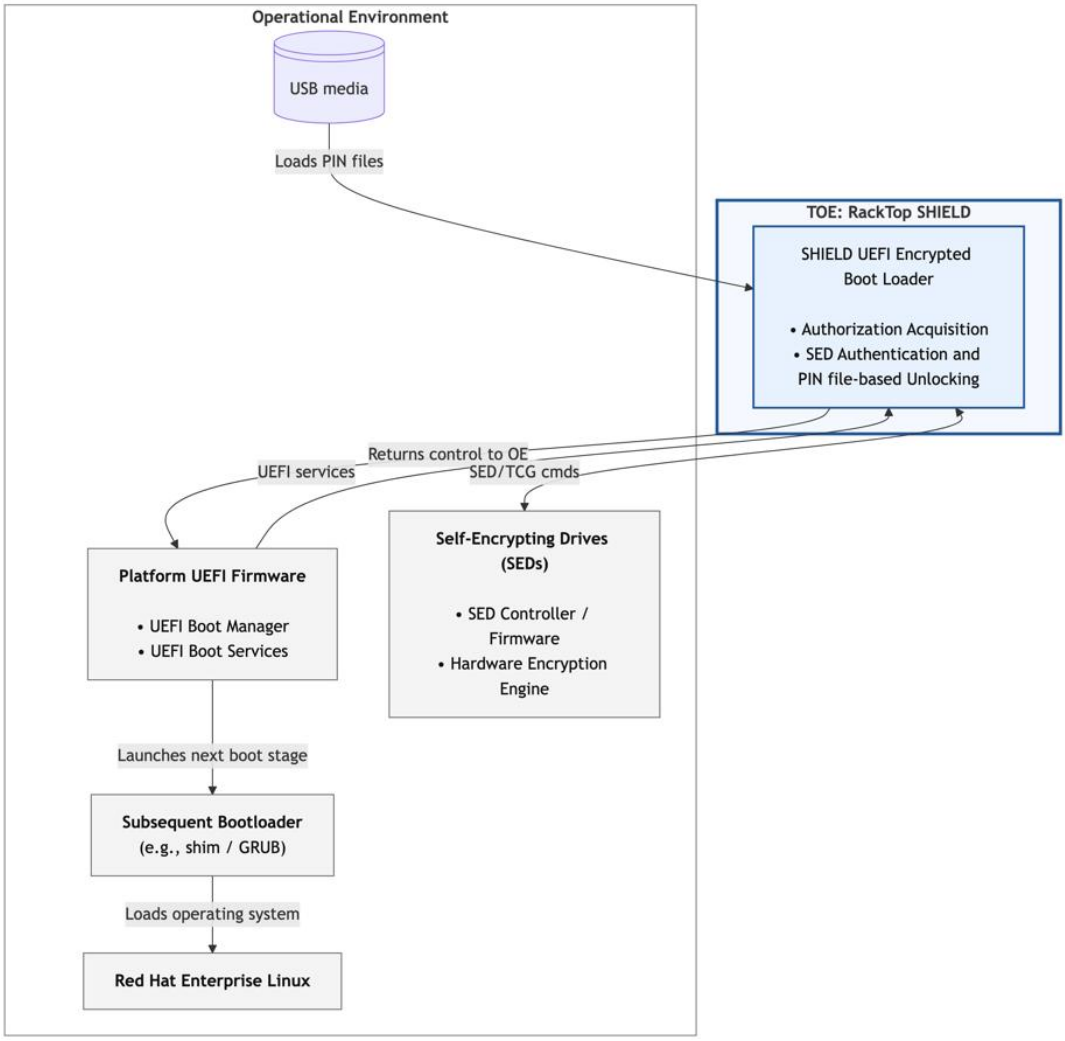
1.6.1 Physical Scope

The Target of Evaluation (TOE) is comprised exclusively of the eboot UEFI application and it's supporting runtime components. The TOE executes during the early boot phase, prior to the initialization of the operating system, and is responsible for critical functions related to the secure initialization and unlocking of Self-Encrypting Drives (SEDs).

The TOE is designed to be deployed as the Outer Encryption Layer in a CSfC-compliant two-layer DAR solutions. It is intended for use in mission-critical environments that require high assurance protection of sensitive or classified data at rest. The TOE simplifies deployment of SED-based encryption and facilitates secure key handling without reliance on enterprise key management infrastructure.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Figure 1 – TOE Boundary



The TOE hardware tested configuration details are listed below:

Processor: Intel(R) Xeon(R) D-2796NT CPU @ 2.00GHz

Motherboard: Supermicro X12SDV-20C-SPT8F

Operating system: RHEL v9.4

Crypto module: OpenSSL 3.x with FIPS provider 3.0.7

OS Drive: DIGISTOR 2TB fw: ECPG13.0

Data Drive: XP12800LE70025 fw: SE4SA54T

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.6.1.1 Guidance Documentation

Table 2 lists the TOE Guidance Documentation needed to install, configure, and maintain the TOE.

Table 2 – Guidance Documentation

Document Name	Description
RackTop Guidance Documentation Supplement Version 0.8	Contains information regarding the specific configuration for the TOE evaluated configuration.

1.6.2 TOE Delivery

Customers will be able to download the TOE ISO from the following website:
URL: https://www.racktopsystems.com/shield

TOE ISO filename: rhel-9-CSFC-20260626-d01c26e7.iso
SHA-256 hash value: 5ba29fb776be50bfe9d94827afef53d5264f832d20c30d1ee9f3c98667be3af6

The TOE installation is performed remotely through a web browser via a management user interface exposed through the Baseboard Management Controller (BMC).

BMC Usage in the TOE evaluated configuration
The BMC is used solely to facilitate initial provisioning and installation of the operational environment. Following completion of operating system installation and system initialization, the BMC shall not remain network accessible.

The TOE RPMs are listed below:

- encrypted-boot-1.1.0_rel.55-1.el9.x86_64.rpm
- updatefde-1.0.2-44.el9.noarch.rpm
- shieldadm-1.0.0-10.el9.x86_64.rpm

Customers will be able to download the TOE documentation from the following website:
https://www.myracktop.com

Users would need to reach out to RackTop to have an account provisioned for them to access the website.

1.6.3 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes, which are further described in sections 7 and 8 of this ST.

- Cryptographic Support
- Security Management
- Protection of the TSF

1.6.3.1 Cryptographic Support

The TOE performs cryptographic operations as specified in Table 8. The TOE has CAVP certificates as indicated in Table 8.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.6.3.2 Security Management

The TOE provides authorized users to update the TOE software. The TOE updates are signed using RSA algorithm by RackTop and verified by the TOE prior to installation.

1.6.3.3 Protection of the TSF

The TOE ensures that all user and system data is encrypted at all times via hardware based FDE. It prevents Operating System boot and drive access until authorized credentials are supplied via external media. Keys are stored on removable media and not present during normal system operation, enhancing offline protection.

1.6.4 Product Physical/Logical Features and Functionality not included in the TOE

- Operating System
- The TOE does not provide its own entropy source for encryption key generation.
- Self-Encrypting Drives (SEDs)

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2. Conformance Claims

This section provides the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in section 9.1.

Table 3 – CC and PP Conformance

CC Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017; CC Part 2 extended; CC Part 3 conformant and no interpretations apply to the claims made in this ST.
PP Identification	Exact Conformance [1] to the *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, 4 Version 2.0 + Errata 20190201, February 1, 2019*. (FDE AA)

Table 4 – NIAP FDE AA Technical Decisions

Technical Decisions	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0458 - FIT Technical Decision for FPT_KYP_EXT.1 evaluation activities	Yes	N/A
TD0606 - FIT Technical Recommendation for Evaluating a NAS against the FDE AA and FDEE	Yes	N/A
TD0759 - FIT Technical Decision for FCS_AFA_EXT.1.1	Yes	N/A
TD0760 - FIT Technical Decision for FCS_SNI_EXT.1.3, FCS_COP.1(f)	Yes	N/A
TD0765 - FIT Technical Decision for FMT_MOF.1	Yes	N/A
TD0766 - FIT Technical Decision for FCS_CKM.4(d) Test Notes	Yes	N/A
TD0767 - FIT Technical Decision for FMT_SMF.1.1	Yes	N/A
TD0769 - FIT Technical Decision for FPT_KYP_EXT.1.1	Yes	N/A
TD0929 - FIT Technical Decision: Clarification to FCS_PCC_EXT.1.1	Yes	N/A
TD1042 - FIT Technical Decision: Replacing FIPS 186-4 with 186-5	Yes	N/A
TD1046 - FIT Technical Decision: Addition of AES-XTS in FCS_COP.1(g)	No	FCS_COP.1(g) has not been applied to this ST.

[1] Exact Conformance is a type of Strict Conformance such that the set of SFRs and the Security Problem Definition/Objectives are exactly as presented within the accepted FDE AA.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3. Security Problem Definition

This section describes Security Problem Definition derived from the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019. The security problem consists of threats that the TOE must mitigate, Assumptions on the operational environment and security objectives for the Operational Environment.

3.1 Threats

This section details all threats as highlighted in the cPP. A threat consists of a threat agent, an asset and an adverse action of that threat agent on that asset. The threat agents are the entities that put the assets at risk if an adversary obtains a lost or stolen storage device. Threats drive the functional requirements for the target of evaluation (TOE).

3.1.1 T.UNAUTHORIZED _DATA_ACCESS

The cPP addresses the primary threat of unauthorized disclosure of protected data stored on a storage device. If an adversary obtains a lost or stolen storage device (e.g., a storage device contained in a laptop or a portable external storage device), they may attempt to connect a targeted storage device to a host of which they have complete control and have raw access to the storage device (e.g., to specified disk sectors, to specified blocks).

3.1.2 T.KEYING_MATERIAL_COMPROMISE

Possession of any of the keys, authorization factors, submasks, and random numbers or any other values that contribute to the creation of keys or authorization factors could allow an unauthorized user to defeat the encryption. The cPP considers possession of key material of equal importance to the data itself. Threat agents may look for key material in unencrypted sectors of the storage device and on other peripherals in the operating environment (OE), e.g. BIOS configuration, SPI flash.

3.1.3 T.AUTHORIZATION_GUESSING

Threat agents may exercise host software to repeatedly guess authorization factors, such as passwords and PINs. Successful guessing of the authorization factors may cause the TOE to release BEV or otherwise put it in a state in which it discloses protected data to unauthorized users.

3.1.4 T.KEYSPACE_EXHAUST

Threat agents may perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms and/or parameters allow attackers to exhaust 3 the key space through brute force and give them unauthorized access to the data.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3.1.5 T.UNAUTHORIZED_UPDATE

Threat agents may attempt to perform an update of the product which compromises the security features of the TOE. Poorly chosen update protocols, signature generation and verification algorithms, and parameters may allow attackers to install software and/or firmware that bypasses the intended security features and provides them unauthorized access to data.

3.2 Assumptions

This section details all assumptions that must remain true in order to mitigate the threats.

3.2.1 A.INITIAL_DRIVE_STATE

Users enable Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption. The cPP does not intend to include requirements to find all the areas on storage devices that potentially contain protected data. In some cases, it may not be possible - for example, data contained in "bad" sectors. While inadvertent exposure to data contained in bad sectors or un-partitioned space is unlikely, one may use forensics tools to recover data from such areas of the storage device. Consequently, the cPP assumes bad sectors, un-partitioned space, and areas that must contain unencrypted code (e.g., MBR and AA/EE pre-authentication software) contain no protected data.
[OE.INITIAL_DRIVE_STATE]

3.2.2 A.SECURE_STATE

Upon the completion of proper provisioning, the drive is only assumed secure when in a powered off state up until it is powered on and receives initial authorization.
[OE.POWER_DOWN]

3.2.3 A.TRUSTED_CHANNEL

Communication among and between product components (e.g., AA and EE) is sufficiently protected to prevent information disclosure. In cases in which a single product fulfils both cPPs, then the communication between the components does not extend beyond the boundary of the TOE (e.g., communication path is within the TOE boundary). In cases in which independent products satisfy the requirements of the AA and EE, the physically close proximity of the two products during their operation means that the threat agent has very little opportunity to interpose itself in the channel between the two without the user noticing and taking appropriate actions.
[OE.TRUSTED_CHANNEL]

3.2.4 A.TRAINED_USER

Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform.
[OE.PASSPHRASE_STRENGTH, OE.POWER_DOWN, OE.SINGLE_USE_ET, OE.TRAINED_USERS]

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3.2.5 A.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_STATE]

3.2.6 A.SINGLE_USE_ET

External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
[OE.SINGLE_USE_ET]

3.2.7 A.POWER_DOWN

The user does not leave the platform and/or storage device unattended until all volatile memory is cleared after a power-off, so memory remnant attacks are infeasible. Authorized users do not leave the platform and/or storage device in a mode where sensitive information persists in non-volatile storage (e.g., lock screen). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.
[OE.POWER_DOWN]

3.2.8 A.PASSWORD_STRENGTH

Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.
[OE.PASSPHRASE_STRENGTH]

3.2.9 A.PLATFORM_I&A

The product does not interfere with or change the normal platform identification and authentication functionality such as the operating system login. It may provide authorization factors to the operating system's login interface, but it will not change or degrade the functionality of the actual interface.
[OE.PLATFORM_I&A]

3.2.10 A.STRONG_CRYPTO

All cryptography implemented in the Operational Environment and used by the product meets the requirements listed in the cPP. This includes generation of external token authorization factors by a RBG.
[OE.STRONG_ENVIRONMENT_CRYPTO]

3.2.11 A.PHYSICAL

The platform is assumed to be physically protected in its Operational Environment and not subject to physical attacks that compromise the security and/or interfere with the platform’s correct operation.
[OE.PHYSICAL]

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3.3 Organizational Security Policy

There are no organizational security policies addressed by this cPP.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4. Security Objectives

4.1 Security Objectives for the Operational Environment

The following subsections describe objectives for the Operational Environment.

4.1.1 OE.TRUSTED_CHANNEL

Communication among and between product components (i.e., AA and EE) is sufficiently protected to prevent information disclosure.

4.1.2 OE.INITIAL_DRIVE_STATE

The OE provides a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption.

4.1.3 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.

4.1.4 OE.POWER_DOWN

Volatile memory is cleared after power-off so memory remnant attacks are infeasible.

4.1.5 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.

4.1.6 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.

4.1.7 OE.TRAINED_USERS

Authorized users will be properly trained and follow all guidance for securing the TOE and authorization factors.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4.1.8 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.

4.1.9 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.

4.1.10 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.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5. Extended Components

Extended components defined in this ST have been drawn directly from FDE_AA cPP. Refer to the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.for further details.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6. Security Assurance Requirements

The cPP identifies the SARs to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

This section lists the set of SARs from CC3.1 Revision 5 that are required in evaluations against the FDE AA cPP. Individual Evaluation Activities to be performed are specified in the Supporting Document (Mandatory Technical Document) Full Drive Encryption: Authorization 6 Acquisition, February 2019.

The general model for evaluation of TOEs against STs written to conform to the cPP is as follows: after the ST has been approved for evaluation, the ITSEF[2] will obtain the TOE, supporting environmental IT (if required), and the guidance documentation for the TOE. The ITSEF is expected to perform actions mandated by the Common Evaluation Methodology (CEM) for the ASE and ALC SARs. The ITSEF also performs the Evaluation Activities contained within the SD, which are intended to be an interpretation of the other CEM assurance requirements as they apply to the specific technology instantiated in the TOE. The Evaluation Activities that are captured in the SD also provide clarification as to what the developer needs to provide to demonstrate the TOE is compliant with the FDE AA cPP.

The TOE security assurance requirements are identified in Table 5.

Table 5 – Security Assurance Requirements

Assurance Requirements	
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM[3] coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – sample (ATE_IND.1)
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.1)

[2] ITSEF – Information Technology Security Evaluation Facility
[3] CM – Configuration Management

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7. Security Functional Requirements

The individual security functional requirements are specified in the following sections. SFRs in this section are mandatory SFRs that any conformant TOE must meet. Based on selections made in these SFRs, it will also be necessary to include some of the selection-based SFRs in Appendix B. Additional optional SFRs may also be adopted from those listed in Appendix A.

The Evaluation Activities defined in the [SD] describe actions that the evaluator will take in order to determine compliance of a particular TOE with the SFRs. The content of these Evaluation Activities will therefore provide more insight into deliverables required from TOE Developers.

7.1 Conventions

The conventions used in descriptions of the SFRs are as follows:

- Assignment: Indicated with italicized text surrounded by brackets (e.g., [*assignment*]).
- Refinement made in the PP: Indicated with bold text and strikethroughs (e.g., "**refinement**" or "~~refinement~~").
- Selection: Indicated with underlined text surrounded by brackets (e.g., [selection]).
- Assignment within a selection: Indicated with italicized and underlined text surrounded by brackets (e.g., [*assignment within a selection*]);

7.2 Security Functional Requirements

This section specifies the SFRs for the TOE and organizes the SFRs by CC class. Table 6 identifies all SFRs implemented by the TOE and indicates the ST operations made by the ST author performed on each requirement. Refinements made in the PP are also indicated.

Table 6 – TOE Security Functional Requirements

Name	Description	S	A	R
FCS_AFA_EXT.1	Authorization Factor Acquisition	✓		
FCS_AFA_EXT.2	Timing of Authorization Factor Acquisition			
FCS_CKM.4(a)	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.4(b)	Cryptographic Key and Key Material Destruction (Power Management)			✓
FCS_COP.1(a)	Cryptographic Operation (Signature Verification)	✓	✓	✓
FCS_COP.1(b)	Cryptographic Operation (Hash Algorithm)	✓	✓	✓
FCS_KYC_EXT.1	Key Chaining (Initiator)	✓	✓	
FCS_SNI_EXT.1	Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)	✓		
FMT_MOF.1	Management of Functions Behavior	✓	✓	✓
FMT_SMF.1	Specification of Management Functions	✓	✓	✓
FMT_SMR.1	Security Roles	✓		
FPT_KYP_EXT.1	Protection of Key and Key Material	✓		

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R
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	✓	✓	✓

Note: S=Selection; A=Assignment; R=Refinement;

7.2.1 Class FCS: Cryptographic Support

FCS_AFA_EXT.1 Authorization Factor Acquisition

FCS_AFA_EXT.1.1

The TSF shall accept the following authorization factors: [

• an external USB token factor that is at least the same security strength as the BEV and is providing a submask generated by the Host Platform].

FCS_AFA_EXT.2 Timing of Authorization Factor Acquisition

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.

FCS_CKM.4(a) Cryptographic Key Destruction (Power Management)

FCS_CKM.4.1(a) Refinement: The TSF shall [**instruct the Operational Environment to clear**] **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)].*

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

FCS_CKM.4.1(d) Refinement: 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 [***
    - o ***removal of power to the memory,***

]

that meets the following: [*no standard*].

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

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

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

FCS_CKM_EXT.4.1(b) Refinement: 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**.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FCS_COP.1(a) Cryptographic Operation (Signature Verification)

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

- ***RSA Digital Signature Algorithm with a key size (modulus) of [3072-bit, 4096-bit];***

]

that meet the following: [

- ***FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5, using PKCS #1 v2.2 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***

].

TD1042 has been applied.

FCS_COP.1(b) Cryptographic Operation (Hash Algorithm)

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

FCS_KYC_EXT.1 Key Chaining (Initiator)

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

- one, using a submask as the BEV;

] .

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 [*the SED*] [

- without validation taking place].

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

FCS_SNI_EXT.1.1 The TSF shall [use no salts].

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

FCS_SNI_EXT.1.3 The TSF shall [use no IVs].

TD0760 has been applied.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7.2.2 FMT_MOF.1 Management of Functions Behavior

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*].

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 Refinement: 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 values or set of authorization values used within the supported authorization method,
d) initiate TOE firmware/software updates,
e) ***[no other functions]****.*

TD0767 has been applied.

FMT_SMR.1 Security Roles

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.

7.2.3 Protection of the TSF (FPT)

FPT_KYP_EXT.1 Protection of Key and Key Material

FPT_KYP_EXT.1.1 The TSF shall [
only store plaintext keys that meet any one of the following criteria [
o the non-volatile memory the key is stored on is located in an external storage device for use as an authorization factor,]].

FPT_PWR_EXT.1 Power Saving States

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

FPT_PWR_EXT.2 Timing of Power Saving States

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].

FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1
The TSF shall run a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF: [*FIPS power-on self-tests*].

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FPT_TUD_EXT.1 Trusted Update

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

FPT_TUD_EXT.1.2 Refinement: The TSF shall provide [*authorized users*] the ability to initiate updates to TOE **[software]** ~~software/firmware~~.

FPT_TUD_EXT.1.3 Refinement: 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.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

8.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 7 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Function	SFR	Description
Cryptographic Support	FCS_AFA_EXT.1	Authorization Factor Acquisition
	FCS_AFA_EXT.2	Timing of Authorization Factor Acquisition
	FCS_CKM.4(a)	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.4(b)	Cryptographic Key and Key Material Destruction (Power Management)
	FCS_COP.1(a)	Cryptographic Operation (Signature Verification)
	FCS_COP.1(b)	Cryptographic Operation (Hash Algorithm)
	FCS_KYC_EXT.1	Key Chaining (Initiator)
	FCS_SNI_EXT.1	Cryptographic Operation (Salt, Nonce, and Initialization Vector Generation)
Security Management	FMT_MOF.1	Management of Functions Behavior
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	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

8.1.1 Cryptographic Support

Table 8 - CAVP Algorithm Certificate References

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Algorithm	Description/Operation	Supported Mode / Standard	Key Sizes	CAVP Cert. #	SFR
RSA	Signature Verification	FIPS PUB 186-5	3072 bits 4096 bits	A8190	FCS_COP.1(a)
SHA	Cryptographic hashing services	ISO/IEC 10118-3:2004	512 bits	A8190	FCS_COP.1(b)

NOTE: Please refer to the KMD (Key Management Description) for SHIELD v1.0 (January 13, 2026) for the description of the Key Management details.

FCS_AFA_EXT.1, FCS_AFA_EXT.2
The TOE accepts keys via an external USB token as the only authorization factor. Keys used to authenticate and unlock SEDs, commonly referred to as PINs are files containing 256-bit binary blobs. These files reside at the root of the externally attached USB storage media. This media is normally physically removed from the system, which is the primary means by which the keys are protected. The keys are otherwise stored in their raw form and are presented to the drives verbatim without any further modification or combining. A utility is used to generate initial set of keys at the time of SED enrollment and for all subsequent re-key operations where the existing authorization key (PIN) is replaced with a new randomly generated key. The system cannot proceed with boot until all drives are unlocked. The token contains the same security strength as the Border Encryption value and the submask is provided by the OS.

The TOE reacquires 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 plain text data. Transitioning from a compliant power saving state destructs all keys from volatile memory.

FCS_CKM.4(a)
There are two operating modes which must be addressed. In the pre-boot environment, the eboot early stage bootloader reads keys from external media into volatile memory. In user space, management utilities read keys from external media and generate keys via the OE DRBG, in both cases placing them into volatile memory for periods of time. The early-stage bootloader as a necessary precaution zeroes out the memory which previously contained key material as soon as the keys are not required.

In user space, management utilities as a necessary precaution zero out memory which previously contained key material as soon as the keys are not required.

FCS_CKM.4(d)
The only volatile memory available to the TOE is the host system's Random Access Memory (RAM). It is the primary working memory which the TOE components utilize to operate on keys.

Volatile key material exists only transiently in system memory during specific operational activities. In all cases, key material is held exclusively in RAM and is erased upon entry into a compliant power-saving or power-off state, during which system memory is cleared.

In all operational contexts including PIN rotation and drive unlocking, volatile key material is retained in memory only for the minimum duration necessary to perform its intended function. Memory buffers containing key material are explicitly cleared by writing zeros over the allocated buffers before the memory is freed immediately after use. Any key material remaining in volatile memory is destroyed upon transition to a compliant power state, ensuring complete sanitization of volatile cryptographic material.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The keys are cleared from memory when the power is removed from the TOE. There is no time where there will be a non-conformance with respect to key destruction.

FCS_CKM_EXT.4(a)
The keys used to authenticate and unlock SEDs are used directly as the BEVs, and they are no longer needed in the early boot context as soon as they are used to authenticate with the SED.
The TOE destroys all keys and key material when no longer required.

FCS_CKM_EXT.4(b)
The only compliant power saving state is shutdown, G2(S5) and G3. All keys in volatile memory are cleared as per FCS_CKM.4(d) when entering a Compliant power saving state.

FCS_COP.1(a)
RSA algorithm is used for signature verification and supports key sizes of 3072 and 4096 bits conforming to FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5, using PKCS #1 v2.2 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. The RSA algorithm is used for signing trusted updates.

The TOE software update mechanism leverages cryptographic signing to verify the authenticity of all packages included in the update bundle in advance of the installation of any packages. Packages are installed *only after* all necessary checks are passed, ensuring authenticity and trusted source of the packages. Software updates are delivered as a bundle of platform-specific RPM packages. (which are themselves cpio archives) wrapped together into a TAR archive. A cpio archive is a file format used to store a collection of files and directories. The public key with which to verify the signature will be provided separately and the RSA key pair may be unique per customer. The location of the TAR archive on the filesystem is not important, but the recommended location is /var/tmp/updates. The authorized administrator will be responsible for transferring the update to the system, which may be accomplished securely via SSH.

The following files are required for the validation of the software packages in the bundle:

Table 9– Files required for validation of the software package

Files	Descriptions
Metadata	Acts as a manifest and includes the name of each package in the bundle as well as the package's SHA-512 checksum.
Signature	Signature file contains the signature of the metadata file included in the bundle. The signature file contains RSASSA-PKCS1-v1_5 formatted binary payload.
RPM	Update bundle package content

The validation process is as follows:

1. Unpack the tarball and read the contents of the metadata and the signature files into memory.
2. Read the contents of the separately provided public key into memory. If the key is missing or there is a problem with the key, the update process is terminated with an error.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3. Perform signature validation of the metadata file with the separately provided public key. If signature check fails, the update process is terminated with a signature validation error.
4. Parse contents of the metadata file and build a set of RPM packages and their corresponding checksums.
5. If the manifest contents do not match exactly with the provided RPMs, the update process is terminated with a validation error.
6. For each RPM file in the manifest, generate a SHA-512 digest and compare the value of the digest against the recorded digest in the metadata file. If there is a mismatch in the hash value between the calculated hash and the value recorded in the metadata file, the update process is terminated with a validation error.
7. After all RPMs have been validated, they are installed via the `dnf` system command.

FCS_COP.1(b)
SHA-512 hash algorithm is used to perform hashing operation conforming to ISO/IEC 10118-3:2004. The hashing algorithms are used for digital signature verification.

FCS_KYC_EXT.1
The TOE provides a 256-bit BEV to the SEDs. All keys stored as files on external USB token act as BEVs and are presented to SEDs without any chaining, i.e. length of chain is one.

FCS_SNI_EXT.1
Salts and nonces are not used by the TOE. IVs are unsupported by the TOE.

8.1.2 Security Management

FMT_MOF.1
The TOE only supports two compliant-power saving states: G2(S5), G3. These power saving states must not be modified while the TOE is configured in the evaluated configuration. Any modifications to this supported configuration will make the system non-compliant. The supported power saving states are normally controlled through the BIOS setup program, which must be configured to prevent unauthorized access, limiting access to authorized administrators only. Only authorized administrators who possess access to the system either via console or remote shell through SSH are allowed to execute the reboot and shutdown commands thereby transitioning the system between compliant states.

FMT_SMF.1, FMT_SMR.1
The TOE implements all required management functions. The TOE itself does not implement DEK changes and erasure because it does not provide the encryption engine itself, rather it facilitates these cryptographic operations. In the TCG Opal Security Subsystem Class (SSC), the GenKey method is a TCG-defined command used to instruct the drive to generate a new random encryption key (internally and atomically) for a given locking object (e.g., Locking Range 0).

The TOE implements necessary interfaces to change or erase the DEK via the TCG-defined GenKey method
a) The DEK is changed with the `shieldadm change-key` command from the running operating system.
b) The DEK is erased with the `\efi\Racktop\eboot.efi-e` command from the UEFI shell.
c) Authorization factors in use cannot be changed; however new values may be set for the drive authorization PINs. The `shieldadm change-pins` command from the running operating system is used for setting the authorization factor values.
d) Software updates are performed with the `updatefde` command from the running operating system.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Only authorized users are permitted access to the TOE.

8.1.3 Protection of the TSF

FPT_KYP_EXT.1
The TOE stores plaintext keys in non-volatile memory which is located on an external USB token for use as an authorization factor.

FPT_PWR_EXT.1
The following compliant savings states are supported: G2(S5) and G3. These states are defined by the Advanced Configuration Power Interface (ACPI) standard. The TOE will enter a Compliant power savings state during a shutdown operation.

FPT_TST_EXT.1.1
The TOE shall run a suite of self-tests during initial start-up (on power on) to demonstrate the correct operation of the TOE. The following self-tests are executed:

Power on self-tests:
- SHA-512 KAT
- DRBG KAT

Conditional tests:
- RSA Sig Verify 3072 KAT
- RSA Sig Verify 4096 KAT

In userspace the OpenSSL cryptographic module provides the TOE with all the necessary cryptographic services. The OpenSSL module at the time of its initial installation executes a suite which includes several Known Answer Tests some of which cover algorithms which the TOE depends upon. This happens once only, and if there are any failures, the installation of the OpenSSL package fails. Each time the FIPS provider module is loaded, before its algorithms are available to the calling application, the module performs pre-operational self-tests and conditional self-tests. No services provided by the module are available while the tests are running. The module does not return control to the calling application until after the tests are successful and module is allowed to remain operational.

FPT_TUD_EXT.1
Only authorized users are permitted to update the TOE. The TOE updates are signed using RSA algorithm by RackTop and verified by the TOE prior to installation. The TOE trusted updates are signed using either RSA 3072 or 4096 bit keys by RackTop and verified by the TOE prior to installation. The TOE does not support automatic update credentials. The TOE version can be queried by issuing the following commands:

```
dnf info encrypted-boot
dnf info updatefde
dnf info shieldadm
```

The RPM output should be the following:

• encrypted-boot-1.1.0_rel.55-1.el9.x86_64.rpm
• updatefde-1.0.2-44.el9.noarch.rpm
• shieldadm-1.0.0-10.el9.x86_64.rpm

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9. Rationale

9.1 Conformance Claims Rationale

This Security Target conforms to Common Criteria Standard for Information Technology Security Evaluations, Version 3.1, Revision 5, April 2017; CC Part 2 extended; CC Part 3 conformant. This ST conforms to the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019.

9.1.1 Variance Between the PP and this ST

There is no variance between the FDE AA cPP and this ST.

9.1.2 Security Assurance Requirements Rationale

This ST claims exact conformance to the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019, including the assurance requirements listed in Section 6 of the FDE AA cPP.

9.1.3 Dependency Rationale

The SFRs in this Security Target represent the SFRs identified in the FDE AA cPP. As such, the FDE AA SFR dependency rationale is deemed acceptable since the PP itself has been validated.

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

10. Acronyms and Terms

10.1 Acronyms

Table 10 – Acronyms

Acronym	Definition
GCM	Galois/Counter Mode
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DRBG	Deterministic Random Bit Generator
FIPS	Federal Information Processing Standard
IT	Information Technology
OSP	Organizational Security Policy
PP	Protection Profile
PUB	Publication
RBG	Random Bit Generator
RHEL	Red Hat Enterprise Linux
RSA	Ron Rivest, Adi Shamir and Leonard Adleman
SAR	Security Assurance Requirement
SED	Self-Encrypting Drive
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SP	Special Publication
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UEFI	Unified Extensible Firmware Interface

©2026 RackTop Systems
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Prepared by:
Corsec Security, Inc.



12600 Fair Lakes Circle, Suite 210
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com