Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

RackTop SPEAR v1.0

Version 1.0, 2 November 2026

Document reference: AISEP-CC-CR-2026-EFT-T066-CR-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary **1**

Introduction **2**

Overview 2

Purpose 2

Identification 2

Target of Evaluation **4**

Overview 4

Description of the TOE 4

TOE Functionality 4

TOE Physical Boundary 4

Architecture 5

Clarification of Scope 6

Security Policy 6

Secure Delivery 6

Version Verification 7

Documentation and Guidance 7

Secure Usage 7

Evaluation **10**

Overview 10

Evaluation Procedures 10

Functional Testing 10

Penetration Testing 10

Certification **12**

Overview 12

Assurance 12

Certification Result 12

Recommendations 12

Annex – References and Abbreviations **14**

References 14

Abbreviations 15

Executive Summary

This report describes the findings of the IT security evaluation of RackTop Systems RackTop SPEAR v1.0 product against Common Criteria approved *Protection Profiles (PPs).*

This report concludes that the Target of Evaluation (TOE) has complied with the following *PPs [4]*:

- *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_AA_V2.0E)*
- *collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_EE_V2.0E).*

Additionally, the above PPs can be grouped together using a certified PP-Configuration. This evaluation used the following PP-Configuration [4]:

- *PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine, Version 1.0, 31 May 2024 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0).*

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs with the final *Evaluation Technical Report (ETR) [7]* submitted on 21 October 2026.

With regard to the secure operation of the TOE, the Australian Certification Authority (ACA) recommends:

- The users should make themselves familiar with the guidance provided with the TOE and pay attention to all security warnings.
- Users of the TOE shall ensure that the Baseboard Management Controller (BMC) functionality is disabled following the setup of the TOE, per section 2.2.1 of the *guidance document [6].*
- Users to note that installation of the TOE image is only possible through the BMC, the product environment during the process of installation is not considered a CC compliant environment.
- Users of the TOE shall be aware that losing/forgetting the configured LUKS passphrase will lead to complete loss of access to data on the TOE.
- Once Self-Encrypting Drives (SEDs) are unlocked, SSH may be used to access the inner layer RHEL OS, however no assurance is provided for this functionality.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the *Security Target [8]* and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the TOE.

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the *Common Criteria [1,2,3]* and *Protection Profiles [4]*
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's *Security Target [8]* which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is RackTop SPEAR v1.0.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	RackTop SPEAR v1.0
TOE Type	Full Drive Encryption
Software version	SPEAR v1.0
Security Target	Security Target, RackTop Systems Inc., RackTop SPEAR v1.0, version 1.2, 08 October 2026
Evaluation Technical Report	Evaluation Technical Report 1.0, dated 21 October 2026 Document reference EFT-T066-ETR 1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	▪ collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_AA_V2.0E)

	▪ collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_EE_V2.0E) ▪ PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine, Version 1.0, 31 May 2024 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0).
Developer	RackTop Systems 13454 Sunrise Valley Drive Suite 550 , Herndon, VA 20171 United States of America
Evaluation facility	Teron Labs Level 2, 14 Moore St, Canberra ACT 2601 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The TOE is RackTop SPEAR v1.0, a Full Drive Encryption (FDE) solution including both Authorisation Acquisition (AA) and Encryption Engine (EE) components. It is built on the Linux Unified Key Setup (LUKS) version 2 specification and leverages RHEL version v9.4 running on dedicated hardware. The TOE implements both the Authorisation Acquisition (AA) function and the Encryption Engine (EE) function, as defined in the Full Disk Encryption collaborative Protection Profiles. The bootloader integration with the AA component ensures that the operating system cannot start until valid credentials are successfully presented and verified. When deployed in its intended configuration, the TOE protects both the operating system drive and all data drives, requiring successful unlocking of each protected volume before the OS completes its boot process and any protected data becomes accessible.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.6 of the *Security Target [8].*

TOE Physical Boundary

The boundary of the TOE includes all parts listed in the *Table 1* below:

Part of the TOE	Identification	Description
TOE Software	RackTop SPEAR v1.0	TOE software is distributed as an ISO package. The following ISO installation packages are used for the TOE: ▪ rhel-9-CSFC-20260626-d01c26e7.iso
Security Guidance	RackTop SPEAR Guidance Document Supplement v0.9	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.

Table 1 – Parts Included in the Physical Scope of the TOE

The TOE was evaluated using the hardware and operational-environment configuration identified below. These components provided the platform on which the TOE was installed and tested. However, they do not form part of the TOE physical boundary. Inclusion in the tested configuration does not imply that the component are independently evaluated as part of the TOE.

- **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

Architecture

The TOE may be deployed as a component of a multilayer encryption architecture designed to meet the requirements with the *US NSA's Commercial Solutions for Classified (CSfC) Data-at-Rest (DAR) Capability Package guidance [13].* The TOE provides a software sector-level encryption of a block device by means of the Linux kernel *dm-crypt* driver, with key hierarchy and protection mechanisms as defined by the LUKS version 2 specification, complementing hardware-based encryption solutions provided by self-encrypting drives (SEDs). In such a complementary dual-layer configuration, all user-accessible data within a configured locking range is encrypted independently by both the SED and the TOE. This layered approach ensures that the compromise or failure of encryption in one layer does not result in the exposure of sensitive information. The TOE implements both the Authorisation Acquisition (AA) function and the Encryption Engine (EE) function, as defined in the Full Disk Encryption collaborative Protection Profiles. The bootloader integration with the AA component ensures that the operating system cannot start until valid credentials are successfully presented and verified. When deployed in its intended configuration, the TOE protects both the operating system drive and all data drives, requiring successful unlocking of each protected volume before the OS completes its boot process and any protected data becomes accessible

Please visit *https://www.nsa.gov* for more information on CSfC Capability Packages.

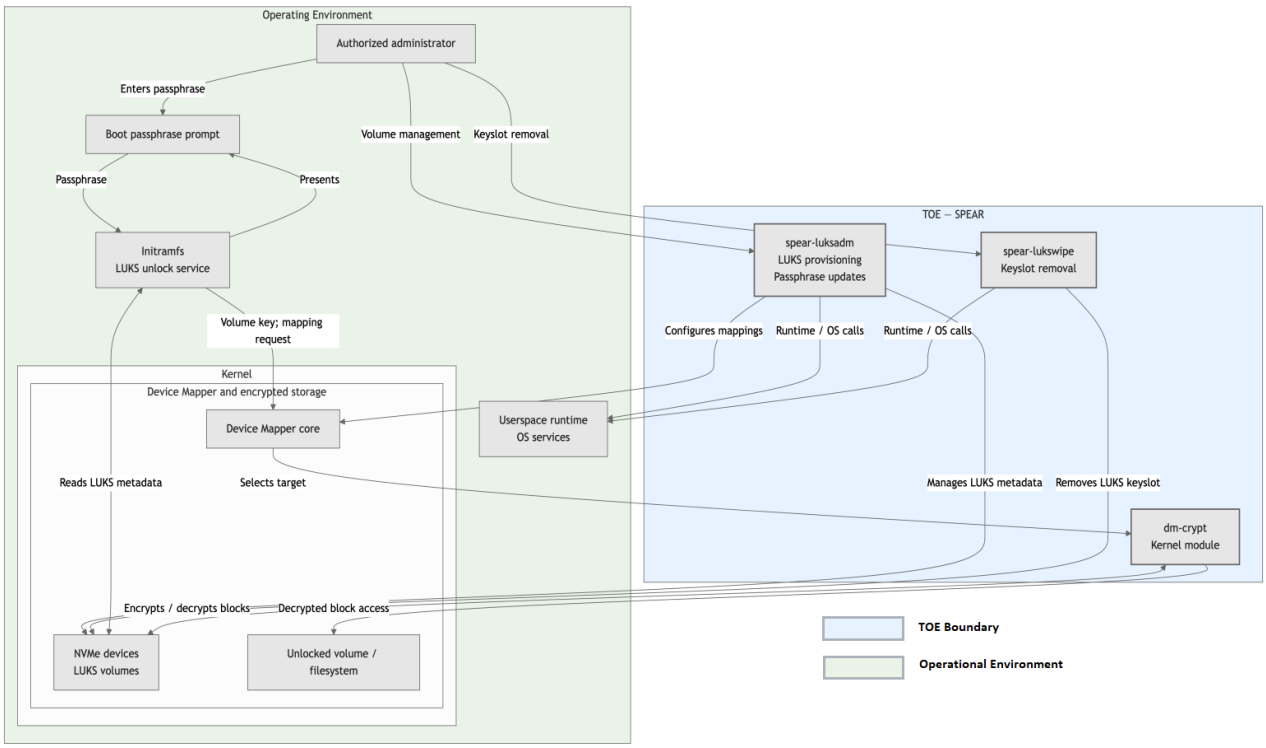


Figure 1 - TOE Architecture

Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the *Security Target [8].*

Evaluated Functionality

Functional tests performed during the evaluation were taken from the *Protection Profiles [4]* and *Supporting Documents [11]* and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

Non-TOE Hardware/Software/Firmware

The TOE is Full Drive Encryption product. Yet, it does require the following external components to operate securely and as evaluated. These items are outside the TOE boundary and must be present and correctly configured in the operational environment.

- Operating System
- The TOE does not provide its own entropy source for encryption key generation.

Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government and Enterprise users should refer to the *ASD Essentials [14]* for guidance on using the certified product in an enterprise, operational technology or government system. Australian Government users should refer to the *Australian Government Information Security Manual [5]* for policy relating to using an evaluated product in an unevaluated configuration.

Security Policy

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The *Security Target [8]* contains a summary of the functionality that is evaluated.

Secure Delivery

The TOE delivery and installation procedures are described in the *Configuration Guidance [6].* The guidance document outlines the required procedures for obtaining and installing the TOE. The TOE software is delivered electronically through the RackTop Systems website.

Installation of the TOE

The *Configuration Guides [6]* contains all relevant information for the secure configuration of the TOE.

Version Verification

Potential user of the TOE can confirm that they have received the product from RackTop Systems by ensuring they downloaded it from *https://www.racktopsystems.com/spear*.

The exact ISO filename should match "rhel-9-CSFC-20260626-d01c26e7.iso" with SHA2-256 hash "5BA29FB776BE50BFE9D94827AFEF53D5264F832D20C30D1EE9F3C98667BE3AF6".

Additionally, after installation of the product, customers can confirm they have received the correct evaluated version of the product by checking the installed version of the TOE relevant SPEAR RPMs:

- spear-utils-1.0.6-33
- updatefde-1.0.2-44

Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased by the consumer, and it is titled as:

- *Guidance Supplement, RackTop Systems Inc., RackTop SPEAR v1.0, version 0.9, 09 October 2026*

All Common Criteria guidance material is available at *https://www.commoncriteriaportal.org*.

The *Australian Government Information Security Manual* is available at *https://www.cyber.gov.au/ism [5].*

The *ASD Essentials* are available at *https://www.cyber.gov.au/essentials [14].*

Secure Usage

The evaluation of the TOE took into account certain assumptions concerning its operational environment. These assumptions must remain valid to ensure that the TOE is installed, provisioned, configured and operated in accordance with its evaluated configuration and that the applicable security objectives are met. The following assumptions are taken from CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E and are stated regardless of applicability to the TOE. The TOE does not support the use of external tokens for Authorization Acquisition functionality, and only uses passphrase-based authorization.

The TOE and its host platform are assumed to be located within a physically secure operational environment that restricts physical access to authorised personnel. The physical protection provided by the operational environment is expected to prevent physical attacks that could compromise the security of the TOE, interfere with the correct operation of the host platform or provide unauthorised access to the storage devices and associated physical interfaces.

Full Drive Encryption must be enabled only on newly provisioned or appropriately initialised storage devices. Before provisioning the TOE, administrators must ensure that protected data is not present in bad sectors, unpartitioned space, storage areas not targeted for encryption, or areas that must remain unencrypted to support boot or pre-authentication functionality. Data intended to be protected must not be placed on the storage device until the Full Drive Encryption provisioning process has been completed successfully. Where a storage device has previously contained sensitive information, it must be securely sanitised before being provisioned for use with the TOE.

Following successful provisioning, the protected storage device is considered to be in a secure state only while the host platform is powered off and before initial authorisation has been provided following power-on. Once the

platform has been powered on and the TOE has successfully processed an authorisation factor, protected data may become accessible through the operational platform. Administrators and authorised users must therefore ensure that the platform is not left unattended while protected storage remains unlocked.

Communication between the Authorisation Acquisition and Encryption Engine components must remain protected against unauthorised disclosure or modification. Where both components are implemented within the TOE, the communication path must remain within the TOE boundary and must not be redirected through an untrusted external interface. Administrators must not modify the component configuration, communication path or relevant platform settings in a manner that could expose authorisation values, derived keying material or other security-relevant information outside the evaluated TOE boundary.

The host platform is assumed to be free from malware or other unauthorised software that could interfere with the correct operation of the TOE. Administrators must maintain the platform in a trusted state through appropriate security controls, including controlled administrative access, secure configuration management, timely application of authorised updates and the prevention or detection of malicious software. The TOE must not be used where the integrity of the host platform, boot environment or security-relevant software cannot be established.

The host platform is assumed to provide its normal identification and authentication functionality independently of the authorisation factor used by the TOE. The TOE does not replace or reduce the security provided by the platform's operating-system login or other platform identification and authentication mechanisms. Administrators must ensure that platform credentials are suitably strong, protected from unauthorised disclosure and managed in accordance with organisational security policies. Any default platform credentials must be replaced before the TOE is placed into operational service.

Authorised users must follow all instructions contained in the evaluated guidance documentation. Passwords, passphrases and any external authorisation tokens must be protected from unauthorised access, disclosure, modification, duplication or substitution. Passwords and passphrases must not be recorded or stored with the protected storage device or host platform in a manner that would permit an unauthorised person to obtain both the protected device and its authorisation factor.

Authorised administrators must ensure that password and passphrase authorisation factors provide sufficient strength and entropy for the sensitivity of the information being protected. Authorisation factors must comply with the minimum strength, composition and length requirements specified in the evaluated guidance. Administrators must not reduce the applicable password or passphrase policy below the values permitted by the evaluated configuration.

Where an external token is used to store or provide an authorisation factor, the token must be used solely for that purpose. External authorisation tokens must be stored separately from the host platform and protected storage device when not in use. Users must maintain appropriate control over each token throughout its lifecycle and must securely sanitise or destroy the token when it is no longer required. External tokens must not be used for unrelated data storage or other purposes that could expose, modify or interfere with the stored authorisation factor.

The operational environment is assumed to provide any cryptographic functionality and random-bit generation services relied upon by the TOE. These services must satisfy the cryptographic requirements identified in the applicable Protection Profile configuration and must be configured and operated in accordance with the evaluated configuration and security guidance. Administrators must ensure that only the evaluated versions and configurations of the required cryptographic components are used. Where the operational environment generates an external-token authorisation factor, the factor must be generated using an approved random-bit generator that satisfies the applicable cryptographic requirements.

The host platform must remain in the required platform state before and while the TOE performs authorisation acquisition or provides the resulting authorisation value to the Encryption Engine. Administrators must not modify the platform firmware, boot configuration, storage configuration, cryptographic components, power-state settings or other security-relevant configuration in a manner that places the TOE outside its evaluated configuration.

The TOE relies on the transition to an evaluated compliant power state to clear plaintext key material and other sensitive security parameters from volatile memory. Authorised users must not leave the host platform or storage device unattended until the applicable shutdown process has completed, volatile memory has been cleared and the protected storage device has returned to a locked state. A lock screen or other operating-system access control must not be treated as equivalent to powering down the platform or transitioning it into an evaluated compliant power state.

Authorised users must not leave the platform in a sleep, suspend, hibernation or other power-managed state unless that state is expressly identified as compliant in the evaluated Security Target and guidance documentation. Where a power-managed state does not provide the required key-destruction and storage-locking behaviour, that state must not be used. Users must be trained to power off the host platform correctly and to confirm that the shutdown process has completed before leaving the platform unattended.

TOE software updates must be obtained through authorised distribution channels and verified using the evaluated trusted-update mechanism before installation. Administrators must ensure that the update bundle and corresponding verification key originate from an authorised source. An update must not be installed where signature verification, integrity verification or package validation fails. Administrators must also ensure that an update does not introduce a software version, cryptographic component or configuration that falls outside the evaluated configuration.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the relevant *Protection Profile [4]* and *Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 [1, 2].*

Testing methodology was drawn from *Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5 [3]* and relevant *Supporting Documents [11].*

The evaluation was carried out in accordance with the operational procedures of the *Australian Information Security Evaluation Program [10]*.

In addition, the conditions outlined in the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [9]* and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs [12]* were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the *Protection Profiles [4]* and *Supporting Documents [11].* The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the *FDE cPP for the Authorisation Acquisition and Encryption Engine Supporting Documents [11]* that follow a flaw hypothesis methodology. Accordingly, four types of flaw hypotheses have been considered:

- Type 1 - public vulnerabilities
- Type 2 - international Technical Community (iTC) sourced
- Type 3 - evaluation team generated
- Type 4 - tool generated.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the TOE and terms relating to the device type of the TOE. These searches were conducted up to the **22 July 2026** coinciding with the conclusion of the evaluation. There were four identifiable Type 2 hypotheses for this evaluation, one applicable to the TOE.

The evaluators performed the following tests to discover any potential vulnerabilities of the TOE:

- Performing a vulnerability scan on the TOE

- Analysis of the BMC and RHEL interfaces, including tool-generated packet fuzzing vulnerability testing of the TOE as per the *Supporting Document [11].*

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification is focused on the evaluation of product compliance with Protection Profiles that cover the technology area of Full Drive Encryption Authorisation Acquisition and Encryption Engine. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the *PP Supporting Documents [11]* and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the *Protection Profiles (PPs) [4].* PP provide assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that *Security Target [8], guidance documentation [6],* and a basic description of the architecture of the TOE.

Certification Result

Teron Labs **has determined** that the TOE upholds the claims made in the *Security Target [8]* and **has met** the requirements of the Protection Profiles *CPP_FDE_AA_V2.0E [4.a], CPP_FDE_EE_v2.0E [4.b] and PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine [4.c].*

After due consideration of the conduct of the evaluation as reported to the certifiers, and of *the Evaluation Technical Report [7]*, the Australian Certification Authority **certifies** the evaluation of the RackTop SPEAR v1.0 performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the *Security Target [8]* have met the requirements of the FDE AA and EE *Protection Profiles [4].*

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the *Australian Government Information Security Manual [5].*

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, the guidance document is followed, and pay attention to all security warnings, the Australian Certification Authority also recommends:

- Users of the TOE shall ensure that the Baseboard Management Controller (BMC) functionality is disabled following the setup of the TOE, per section 2.2.1 of the *guidance document [6].*

- Users to note that installation of the TOE image is only possible through the BMC, the product environment during the process of installation is not considered a CC compliant environment.
- Users of the TOE shall be aware that losing/forgetting the configured LUKS passphrase will lead to complete loss of access to data on the TOE.
- Once Self-Encrypting Drives (SEDs) are unlocked, the use of SSH may be used via the inner layer RHEL OS, however no assurance is provided for this functionality.

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*
2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*
3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*
4. *Protection Profiles:*
    a) *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_AA_V2.0E)*
    b) *collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_EE_V2.0E)*
    c) *PP-Configuration for Full Drive Encryption – Authorization Acquisition and Full Drive Encryption – Encryption Engine, Version 1.0, 31 May 2024 (CFG_CPP_FDE_AA-CPP_FDE_EE_V1.0).*
5. *Australian Government Information Security Manual: https://www.cyber.gov.au/ism*
6. *Guidance Supplement, RackTop Systems Inc., RackTop SPEAR v1.0, version 0.9, 09 October 2026.*
7. *Evaluation Technical Report RackTop SPEAR Version 1.0, dated 21 October 2026 (Document reference EFT-T066-ETR 1.0)*
8. *Security Target, RackTop Systems Inc., RackTop SPEAR v1.0, version 1.2, 08 October 2026*
9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*
10. *AISEP Policy Manual (APM): https://www.cyber.gov.au/sites/default/files/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf*
11. *Protection Profile Supporting Documents*
    a) *Supporting Document, Mandatory Technical Document, Full Drive Encryption: Authorization Acquisition, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_AA_V2.0E_SD)*
    b) *Supporting Document, Mandatory Technical Document, Full Drive Encryption: Encryption Engine, Version 2.0 + Errata 20190201, 01 February 2019 (CPP_FDE_EE_V2.0E_SD).*
12. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0*
13. *National Security Agency, Commercial Solutions for Classified, Data at Rest Capability Packages: https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/capability-packages/ - data-at-rest*
14. *Australian Government ASD Essentials: https://www.cyber.gov.au/essentials*

Abbreviations

AISEP	Australian Information Security Evaluation Program
AA	Authorisation Acquisition
ACA	Australian Certification Authority
APM	AISEP Policy Manual
ASD	Australian Signals Directorate
BMC	Baseboard Management Controller
CC	Common Criteria
CEM	Common Methodology for Information Technology Security Evaluation
cPP	collaborative Protection Profile
CPU	Central processing unit
CSfC	Commercial Solutions for Classified
DAR	Data-at-Rest
ETR	Evaluation Technical Report
FDE	Full Drive Encryption
FIPS	Federal Information Processing Standard
GHz	Gigahertz
IT	Information Technology
iTC	international Technical Community
OS	Operating System
PDF	Portable Document Format
PP	Protection Profile
RHEL	Red Hat Enterprise Linux
SEDs	Self-encrypting drives
SSH	Secure Shell
SSL	Secure Sockets Layer
TB	Terabyte

TCG- Compliant	Trusted Computing Group Compliant
TOE	Target of Evaluation
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government

Australian Signals Directorate