TLP:WHITE

Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

COMMON CRITERIA CERTIFICATION REPORT

CipherDriveOne 2.0.1

27 June 2024

648-LSS

V1.0

Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Program, and the conclusions of the testing laboratory in the evaluation report are consistent with the evidence adduced.

This report, and its associated certificate, are not an endorsement of the IT product by Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security
Contact Centre and Information Services
contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

OVERVIEW

The Canadian Common Criteria Program provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCTL.

The certification report, certificate of product evaluation and security target are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

CipherDriveOne 2.0.1 (hereafter referred to as the Target of Evaluation, or TOE), from **KLC Group LLC** , was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Section 1.1 for the evaluated security functionality.

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **27 June 2024** and was carried out in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list (CPL) for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	CipherDriveOne 2.0.1
Developer	KLC Group LLC

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

The TOE claims the following conformance:

collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201

1.2 TOE DESCRIPTION

The TOE provides pre-boot user authentication for Opal 2.0 compliant self encrypting drives (SEDs). It is designed to be used with a SED as a coupled system to deliver secure Data-At-Rest (DAR) encryption.

The TOE is installed on a read-only Shadow Master Boot Record (MBR) partition on the SED. After installation, the user authenticates to the TOE which will unlock the SED drive and chain-boot to the protected OS or hypervisor environment.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

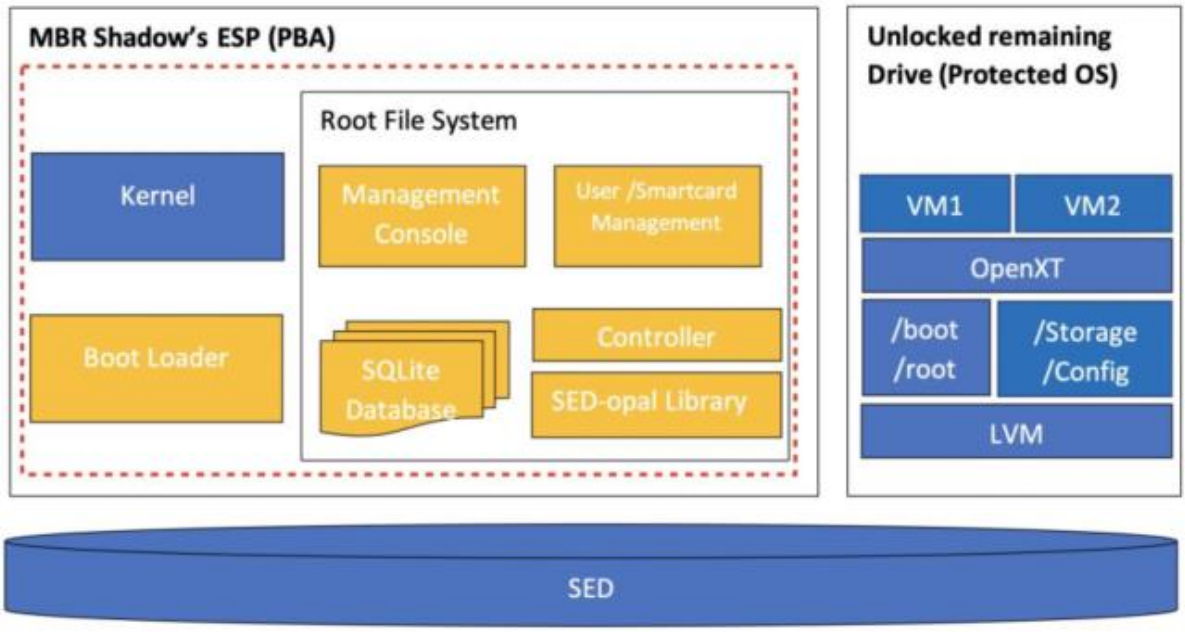


Figure 1: TOE Architecture

2 SECURITY POLICY

The TOE implements and enforces policies pertaining to the following security functionality:

- Cryptographic Support
- Security Management
- Protection of the TSF

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic implementations are used by the TOE and have been evaluated by the CAVP/CMVP:

Table 2: Cryptographic Implementation(s)

Cryptographic Implementation	Certificate Number
OpenSSL 3.2.1 Cryptographic Module	A5187

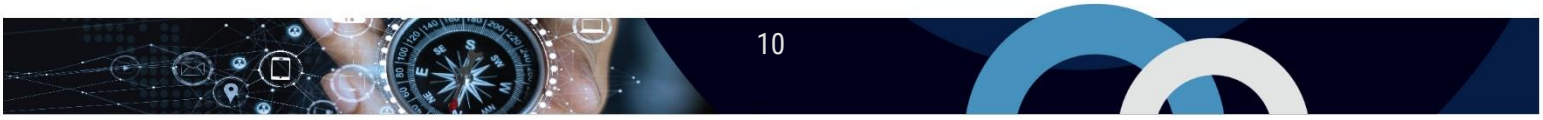
3 ASSUMPTIONS AND CLARIFICATION OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions, as defined in the collaborative Protection Profile (cPP), are made regarding the use and deployment of the TOE:

- 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 unpartitioned 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.
- 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
- 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.
- Authorized users follow all provided user guidance, including keeping password/passphrases and external tokens securely stored separately from the storage device and/or platform.
- 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.
- External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.
- 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".
- Authorized administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.



- 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.
- 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.
- 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.

3.2 CLARIFICATION OF SCOPE

- Only the functionality covered in the collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201 is included within the scope of evaluation.
- The TOE supports Opal 2.0 compliant SEDs but was only evaluated with the specific SEDs listed in Section 4.
- The TOE was only evaluated protecting specific Operating Systems listed in Section 4.
- Use of multiple SEDs on the same system has not been evaluated.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

TOE Software/Firmware	CipherDriveOne 2.0.1 Build: 3
Supported SEDs	• Advantech SQFFCM8V4-256GEC (256GB M.2 NVMe) • Advantech SQFFS25V4-256GSC (256GB 2.5" SATA) • Digistor DIG-SSD25126-SI (512GB 2.5" SATA) • Digistor DIG-M2N25126-UI (512GB M.2 NVMe) • Seagate Barracuda 515 (512GB M.2 NVMe) • Seagate Nytro 5350H XP1920SE70015 (1.92TB 2.5”x15mm U.3 PCIe Gen4 x4 NVMe SED) • Seagate Nytro 5350H XP1920SE70025 (1.92TB 2.5”x15mm U.3 PCIe Gen4 x4 NVMe FIPS 140-3/Common Criteria)
Protected Operating Systems	• Microsoft Windows 10 • Microsoft Windows 11 • Red Hat Enterprise Linux 8 • Red Hat Enterprise Linux 9
Environmental Support	• Intel-based 64-bit system that supports UEFI. ○ Was tested using Intel Core i5-13400 (Raptor Lake) • Federal Information Processing Standard (FIPS) 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smartcards and readers are required.

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a) KLC Group LLC, CipherDriveOne v2.0.1, KLC PBA, 1-25-2024
b) KLC CipherDriveOne 2.0.1 Common Criteria Guide, 1.3

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT TESTING

During this evaluation, the evaluator developed independent functional & penetration tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP

b. Cryptographic Implementation Verification: The evaluator verified that the claimed cryptographic implementations were present in the TOE.

6.3.1 INDEPENDENT TESTING RESULTS

The developer's tests and the independent tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 VULNERABILITY ANALYSIS

The vulnerability analysis focused on 4 flaw hypotheses.

- Public Vulnerability based (Type 1)
- Technical community sources (Type 2)
- Evaluation team generated (Type 3)
- Tool Generated (Type 4)

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases and technical community sources (Type 1 & 2). Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities (Type 4). Based upon this review, the evaluators formulated flaw hypotheses (Type 3), which they used in their vulnerability analysis.

Type 1 & 2 searches were conducted on **24 April 2024** and included the following search terms:

• CipherDriveOne 2.0.1	• Digistor DIG-M2N25126-UI	• Systemd-boot v241
• OpenSSL 3.2.1	• Digistor DIG-SSD25126-SI	• OpenSC v0.25.1
• Linux Kernel 6.6.14	• Barracuda 515	• Nginx: v1.24.0
• Advantech SQFFCM8V4-256GEC	• Seagate Nytro 5350H	• Uwsgi v2.0.18
• Advantech SQFFS25V4-256GSC	• Intel Core i5-13400 (Raptor Lake)	• Qt v5.15.2

Vulnerability searches were conducted using the following sources:

National Vulnerability Database: https://nvd.nist.gov/vuln/search	CCCS – Alerts and advisories: https://cyber.gc.ca/en/alerts-advisories
Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html	OpenSSL Vulnerabilities: https://www.openssl.org/news/vulnerabilities.html
CISA – Known Exploited Vulnerabilities Catalog: https://www.cisa.gov/known-exploited-vulnerabilities-catalog	Nginx Security Advisories: http://nginx.org/en/security_advisories.html
Snyk Security: https://security.snyk.io/	KLC website: https://cipherdriveone.com/

6.4.1 VULNERABILITY ANALYSIS RESULTS

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

This evaluation has provided the basis for the conformance claim documented in Section 1.1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
cPP	Collaborative Protection Profile
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
KLC Group LLC CipherDriveOne 2.0.1 Security Target, v1.3, 26 June 2024
KLC Group LLC CipherDriveOne 2.0.1 Evaluation Technical Report, v1.1, 27 June 2024
KLC Group LLC CipherDriveOne 2.0.1 Assurance Activity Report, v1.1, 27 June 2024