KLC Group LLC

CipherDriveOne Kryptr 1.1.0

Common Criteria Guide

Version 1.1

April 2024

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.0	04 Apr 2024	G Nickel	Release for Check Out
1.1	23 Apr 2024	G Nickel	Address ECR Comments

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions and related information to achieve the Common Criteria evaluated configuration of CipherDriveOne Kryptr 1.1.0

1.2 Audience

2 This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed in Table 3.

1.3 About the Common Criteria Evaluation

3 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

1.3.1 Conformance Claims

1.3.1.1 Common Criteria Conformance

4 The Target of Evaluation subject to this evaluation complies with the following:

a) CC Version 3.1 Revision 5

b) CC Part 2 Extended

c) CC Part 3 Conformant

1.3.1.2 Protection Profile Conformance

5 This Common Criteria evaluation was performed against the requirements of the following Protection Profiles (available at https://www.niap-ccevs.org/Profile/PP.cfm):

a) collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201 (referenced within as CPP_FDE_AA)

b) collaborative Protection Profile for Full Drive Encryption – Encryption Engine, v2.0 + Errata 20190201 (referenced within as CPP_FDE_EE)

c) NIAP Technical Decisions per Table 2 in [ST].

1.3.2 Evaluated Software

6 The Target of Evaluation (TOE) is the KLC CipherDriveOne Kryptr 1.1.0, build 17 software.

7 The TOE is downloaded from a password protected web portal subsequent to purchase.

8 Users may verify that they have the correct version of the TOE by referencing the name and version displayed at the Pre-Boot Authentication Login screen.

1.3.3 Non-TOE Components

9 The TOE operates with the following components in the environment:

a) **Protected OS.** The TOE supports protection of the following Linux Operating Systems and Windows Operating Systems:

i) Red Hat Enterprise Linux 8

ii) Red Hat Enterprise Linux 9

iii) Microsoft Windows 10

iv) Microsoft Windows 11

CC Testing was performed using the following operating systems:

- Red Hat Enterprise Linux 9
- Microsoft Windows 11

b) **Computer Hardware.** 64-bit Intel-based UEFI booted systems that supports Intel Secure Key Technology. CC testing was performed using the following CPUs:

i) Intel Core i7-1265U (Alder Lake)

c) **Smartcard and reader.** When dual factor authentication is used, Federal Information Processing Standard (FIPS) 201 Personal Identity Verification Common Access Card (PIV-CAC) compliant smartcards and readers are required.

1.3.4 Evaluated Functions

10 The following functions have been evaluated under Common Criteria:

a) **Data Protection.** The TOE performs full drive encryption to protect data from unauthorized disclosure.

b) **Secure Key Material.** The TOE ensures key material used for storage encryption is properly generated and protected from disclosure. It also implements cryptographic key and key material destruction during transitioning to a Compliant power saving state, or when all keys and key material are no longer needed.

c) **Secure Management.** The TOE enables management of its security functions.

d) **Trusted Update.** The TOE ensures the authenticity and integrity of software updates through digital signatures using RSA 3072 with SHA-384.

e) **Cryptographic Operations.** The cryptographic operations performed by the TOE have been validated for correct implementation and are described in [ST] Table 12.

11 **NOTE:** No claims are made regarding any other security functionality.

1.3.5 Evaluation Assumptions

12 The following assumptions are defined by the CPP_FDE_AA and CPP_FDE_EE protection profiles. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 1: CPP_FDE_AA Evaluation Assumptions

Assumption	Guidance
A.INITIAL_DRIVE_STATE - Users enable	Drives should be formatted prior to use with

Assumption	Guidance
Full Drive Encryption on a newly provisioned or initialized storage device free of protected data in areas not targeted for encryption	CipherDriveOne Kryptr.
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.	Provisioning of the TOE should be completed per all guidance documents and instructions to ensure nominal operation.
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 this case, CipherDriveOne Kryptr is both the Authorization Acquisition (AA) component, and the Encryption Engine (EE) component. No action is required.
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.	Administrators should be familiar with this document and should ensure that users are trained in using CipherDriveOne Kryptr. Administrators and users must protect passwords and smartcards in accordance with organizational policies.
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.	CipherDriveOne Kryptr does not provide malware protection. OS compatible anti-malware software should be enabled.
A.SINGLE_USE_ET - External tokens that contain authorization factors are used for no other purpose than to store the external token authorization factors.	CipherDriveOne Kryptr may be used with Smart Cards. The Smart Cards should only be used for identification purposes.
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”.	No action is required.
A.PASSWORD_STRENGTH - Authorized	Administrators should ensure that

Assumption	Guidance
administrators ensure password/passphrase authorization factors have sufficient strength and entropy to reflect the sensitivity of the data being protected.	CipherDriveOne Kryptr users are aware of organizational password policies.
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.	The Host OS that boots after unlock should require users to authenticate.
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.	CipherDriveOne Kryptr makes use of OS provided cryptography to perform drive encryption. Operating Systems use with CipherDriveOne Kryptr should have FIPS140 validated cryptography. See https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules
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.	Devices protected by CipherDriveOne Kryptr should be physically protected (during operation) in accordance with organizational policies.

Table 2: CPP_FDE_EE Evaluation Assumptions

Assumption	Guidance
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 this case, CipherDriveOne Kryptr is both the Authorization Acquisition (AA) component, and the Encryption Engine (EE) component. No action is required.
A.INITIAL_DRIVE_STATE - Users enable Full Drive Encryption on a newly provisioned storage device free of protected data in areas not targeted for encryption. It is also assumed that data intended for protection should not be on the targeted storage media	Drives in each device should (preferably) be formatted and (preferably) Host OS installed prior to use with CipherDriveOne Kryptr. However, the following modes are supported. 1) OS is first installed and then PBA is

Assumption	Guidance
until after provisioning.	installed 2) PBA is installed and then OS is installed. (For this, the PBA should remain in deactivated state and should be activated after OS is installed)
A.TRAINED_USER - Users follow the provided guidance for securing the TOE and authorization factors. This includes conformance with authorization factor strength, using external token authentication factors for no other purpose and ensuring external token authorization factors are securely stored separately from the storage device and/or platform. The user should also be trained on how to power off their system.	Administrators should be familiar with this document and should ensure that users are trained in using CipherDriveOne Kryptr. Administrators and users must protect passwords and smartcards in accordance with organizational policies.
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.	CipherDriveOne Kryptr does not provide malware protection. OS compatible anti-malware software should be enabled.
A.POWER_DOWN - The user does not leave the platform and/or storage device unattended until the device is in a Compliant power saving state or has fully powered off. This properly clears memories and locks down the device. 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 or sleep state). Users power the platform and/or storage device down or place it into a power managed state, such as a “hibernation mode”.	No action is required.
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.	CipherDriveOne Kryptr makes use of OS provided cryptography to perform drive encryption. Operating Systems use with CipherDriveOne Kryptr should have FIPS140 validated cryptography. See https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules
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.	Devices protected by CipherDriveOne Kryptr should be physically protected in accordance with organizational policies.

1.4 Related Documents

13 This guide supplements the below documents which are available from KLC's web portal.

Table 3: Related Documents

Reference	Document
[ST]	KLC Group LLC CipherDriveOne Kryptr 1.1.0 Security Target, Version 1.5
[MAN]	KLC Group LLC CipherDriveOne Kryptr Administrator Guide, V 1.0.1, 4-18-2024

14 **NOTE:** The information in this guide supersedes related information in other documentation.

1.5 Terminology

15 Table 4 below defines terms and acronyms used within this document that are not commonly known.

Table 4: Terminology

Term	Definition
AA	Authorization Acquisition
AES	Advanced Encryption Standard
AK	Authentication Key
BEV	Border Encryption Value
BIOS	Basic Input Output System
CBC	Cipher Block Chaining
CC	Common Criteria
CEM	Common Evaluation Methodology
CDO	CipherDriveOne Kryptr
CPP	Collaborative Protection Profile
DAR	Data At Rest
DEK	Data Encryption Key
DRBG	Deterministic Random Bit Generator

Term	Definition
EE	Encryption Engine
EMK	Encrypted Master Key
FIPS	Federal Information Processing Standards
FDE	Full Drive Encryption
KEK	Key Encryption Key
KLC	KLC Group LLC
KMD	Key Management Description
LUKS	Linux Unified Key Setup
Opal 2.0	Trusted Computing Group standard for SEDs.
OS	Operating System
PBKDF2	Password-Based Key Derivation Function
PIV-CAC	Personal Identity Verification Common Access Card
PXE	Preboot eXecution Environment
RBG	Random Bit Generator
RSA	Rivest Shamir Adleman Algorithm
SED	Self-Encrypting Drive
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
XOR	Exclusive OR

2 Guidance

2.1 Host OS Configuration

16 The 'Sleep' power state should be disabled in the Host OS that boots after drive unlock. The compliant power states supported by CipherDriveOne Kryptr are described in section 2.5 below.

17 The following security practices are recommended after installation:

a) Configure a BIOS admin password

b) Disable boot from portable media (e.g., USB)

c) Disable warm boot options such as Fast Startup

2.2 Configuration

18 Follow the instructions in [MAN] section '*Installation of CDO Kryptr'* to install and configure the TOE in accordance with the operating environment.

2.3 Authorization Factors

19 CipherDriveOne Kryptr supports the following authorization factors:

a) **Passwords.** Users authenticate via username and password. See [MAN] *Add a Password User.* **Note:** For the installer command line, special characters (e.g. the $ sign) can be entered in the password section (of the command line) by enclosing the password in single quotes. For example: `sh install-fde.sh -d /dev/sda -p 'My$passwd'`.

b) **Multi-Factor.** Users authenticate via username, password, and smart card**.** Smart Cards must be FIPS201 PIV-CAC compliant. See [MAN] "*Multifactor Authentication (MFA)"* and *"Add a MFA (Multifactor Authentication) User"* for more information.

2.4 Cryptographic Key Destruction

20 CipherDriveOne Kryptr handles the destruction of cryptographic keys and key material when they are no longer required. There are no situations where key destruction would be delayed or prevented.

21 Transitioning to a compliant power saving state also triggers the destruction of any keys or key material stored in plaintext. When a user initiates a request to enter a power saving state, the TOE will also instruct the protected OS to destroy all cryptographic keys and key material from volatile memory. See section 2.5 for more information on supported power saving states.

2.5 Power Saving States

22 CipherDriveOne Kryptr supports the following compliant power saving states:

a) **S4 - Nonvolatile Sleep.** In this state, the system appears to be off and consumes lowest power. While transitioning to this state from higher power, it may save the contents of the volatile memory to a file. When the system restarts, it will load the contents of the file for a quick boot only after CDO is

invoked for authentication/authorization. The S4 power saving state is only supported on Windows platforms. Red Hat systems do not support the S4 power saving state.

b) **G2(S5) – Soft Off.** In this state, the system appears to be off and involves a complete shutdown of the system and following boot process at which point the CipherDriveOne Kryptr PBA will be invoked for authentication and authorization.

c) **G3 – Mechanical Off.** In this state, the system is completely off and it does not consume any power. The system returns to the working state only after a complete reboot of the system at which point CipherDriveOne Kryptr PBA will be invoked for authentication and authorization.

23 An unexpected power loss would result in the G3 power state. When resuming from the above power saving states, users are required to re-authenticate using the same authorization factors as per normal operation.

24 Users interact with the Host OS or hardware platform to enter the above power saving states. The TOE will enter a compliant power saving state immediately and without delay as prompted by the protected OS after a user-initiated request. While this process is expected to complete within several seconds, it is largely dependent on the host OS.

25 Refer to the Host OS guidance for instructions on entering the above power states.

2.6 Management Functions

26 CipherDriveOne Kryptr provides the following management functions as relevant to the Common Criteria Protection Profile:

a) **Request change of DEK.** See [MAN] '*Change DEK'*.

b) **Request cryptographic erase of DEK.** See [MAN] '*Erase Disk'.*
Note: The steps outlined in [MAN] '*Erase Disk'* also apply to performing erase of DEK.

c) **User change of authorization factors.** See [MAN] '*Update Password User'* and '*Update Smartcard User'*.

d) **Initiate firmware/software updates.** See [MAN] '*CDO Kryptr Upgrade'.*

e) **Configure authorization factors.**

i) For password authentication, see [MAN] '*Add a Password User'*

ii) For MFA authentication, see [MAN] '*Add a MFA User'*

2.7 Updating CipherDriveOne Kryptr

27 Software update files must be manually downloaded from the KLC web portal and then copied to a USB drive. The CDO UI is then used to trigger the update from USB.

28 Detailed update instructions are provided at [MAN] '*CDO Kryptr Upgrade'*.

29 Software updates are digitally signed and CipherDriveOne Kryptr automatically verifies the signature prior to installing an update. If signature verification fails the update is aborted and an error message is displayed "PBA Upgrade has failed".

30 On Windows based systems, drivers are signed by Microsoft. On update of these drivers, the Windows platform will verify signatures automatically during each boot

cycle. On Red Hat based systems, integrity checks of the rpm package signature can be performed using the following command:

```
rpm --checksig -v <rpm_pkg>
```

31 Additional information on updating systems via CLI can be found in [MAN] section *'CDO Kryptr Upgrade via CLI'.*

2.8 Cryptography

32 CipherDriveOne Kryptr supports both 256-bit and 128-bit DEKs and BEVs. The product license determines the supported length of DEK. See [MAN] sections '*CDO Kryptr License'* and '*Generate License Request and Import/Upgrade License'.* Additional information on license request files can be found in [MAN] section *'Generate a License Request File'*.

33 No other configuration of cryptographic parameters is possible/required.

2.8.1 Change Authentication Key

34 CDO generates and manages the Authentication Keys (AKs) used to unlock a drive. If an AK is suspected to have been compromised, a Security Officer can refresh the AKs of all users. See [MAN] section '*Change AK'.*

2.9 Importing Users

35 For systems that are not network connected (air-gapped), [MAN] *Import Users* provides instructions for importing a JSON formatted text file (users list/database file) from a USB thumb drive, CD/DVD or external hard drive. **Note:** /mnt is the starting directory for the removable storage containing the users list/database file.

2.10 Disabling Key Recovery

36 Key recovery functionality (export configuration or backup database) can be disabled at install time (using '-n noexport' as one of the command-line parameters) or (if installed) recovery can be administratively disabled at runtime (by unchecking the 'Recovery' configuration item in the Settings Console as the Security Officer).

37 Further details are provided in [MAN] section '*Installation of CDO Kryptr'* subsection *'CDO Kryptr Install Optional Parameters'* subsection '*Install CDO Kryptr with exported configuration file'.*

2.11 Validation

38 CipherDriveOne Kryptr requires a successful validation of the BEV prior to decryption of the drive and allowing access to TSF data after booting or exiting a compliant power saving state.

39 Administrators can configure the threshold of consecutive failed authentication attempts, resulting in validation failure. If this threshold is met, the system will stop responding and require a power cycle or reboot of the system to reset the counter.

40 The failure threshold can be configured to between 1 and 20 attempts by either 'Administrator' or 'Security Officer' roles in the '*Settings* > *Configuration* > *Security'* menu of the administration console. See [MAN] section *'Settings Configuration for Administrator and Security Officer Users'*.