National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

TM

Validation Report
for the
KLC Group LLC CipherDriveOne Kryptr 1.1.0

Report Number: CCEVS-VR-VID11399-2024
Dated: April 29, 2024
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson

Lori Sarem

Chris Thorpe

The MITRE Corporation

Common Criteria Testing Laboratory

Nathan Bennett

Nil Folquer

Kevin Steiner

Lightship Security USA, Inc.

Table of Contents

List of Tables

1. Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) Validation team of the evaluation of KLC Group LLC CipherDriveOne Kryptr 1.1.0 provided by KLC Group LLC. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Lightship Security USA Common Criteria Laboratory (CCTL) in Baltimore, MD, United States of America, and was completed in April 2024. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, all written by Lightship Security (LS). The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements of the:

- collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition, Version 2.0 + Errata 20190201, February 1, 2019 (CPP_FDE_AA_V2.0E) and
- collaborative Protection Profile for Full Drive Encryption - Encryption Engine, Version 2.0 + Errata 20190201, February 1, 2019 (CPP_FDE_EE_V2.0E).

The TOE is KLC Group LLC CipherDriveOne Kryptr 1.1.0. The TOE identified in this VR has been evaluated at a NIAP approved CCTL using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *KLC Group LLC CipherDriveOne Kryptr 1.1.0 Security Target*, Version 1.5, April 2024, and analysis performed by the Validation Team.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile (PP) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Evaluated Product	KLC Group LLC CipherDriveOne Kryptr 1.1.0
Sponsor and Developer	KLC Group LLC 1900 Camden Ave. San Jose, CA 95124
CCTL	Lightship Security USA, Inc. 3600 O'Donnell St., Suite 2 Baltimore, MD 21224
CC Version	*Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5, April 2017.
CEM	*Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, Version 3.1, Revision 5, April 2017.

Item	Identifier
Protection Profile	*collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019 *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019
ST	*KLC Group LLC CipherDriveOne Kryptr 1.1.0 Security Target*, Version 1.5, April 2024
Evaluation Technical Report	*KLC Group LLC CipherDriveOne Kryptr 1.1.0 Evaluation Technical Report*, Version 0.3, April 2024
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Evaluation Personnel	Nathan Bennett, Nil Folquer, and Kevin Steiner
CCEVS Validators	Jenn Dotson, Lori Sarem, and Chris Thorpe

3. Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The KLC Group LLC CipherDriveOne Kryptr 1.1.0 is software that provides full disk encryption including pre-boot user authentication, chain-boot to the host Operating System (OS) and management capabilities to control user access and settings. It applies full drive encryption to protect all locally stored data from unauthorized access, loss, and exposure in the event a protected device is lost or stolen. The TOE has two distinct modules:

a. PBA / Management module. Provides pre-boot authentication and TOE configuration services.
b. Encryption Engine / Driver. Disk encryption for Linux and Windows Operating Systems.

3.1. TOE Evaluated Configuration

The TOE encompasses the KLC Group LLC CipherDriveOne Kryptr 1.1.0 software (including Linux Kernel 5.15).

3.2. Required Non-TOE Hardware, Software, and Firmware

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:
    a. Red Hat Enterprise Linux 8
    b. Red Hat Enterprise Linux 9
    c. Microsoft Windows 10
    d. Microsoft Windows 11

    CC Testing was performed using the following operating systems:

    a. Red Hat Enterprise Linux 9
    b. 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:
    a. 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.

4. Security Policy

This section summarizes the security functionality of the TOE:

4.1. User Data Protection

The TOE performs full drive encryption on all storage devices to protect data from unauthorized disclosure in the event of loss or theft of the device. All protected data is encrypted by default without user intervention and with NIST approved algorithms.

4.2. Security Management

The TOE provides dedicated interfaces for the management of its security functions. Access to these management functions can be controlled by way of role-based group assignment to administrative users.

4.3. Protection of the TSF

The TOE ensures the authenticity and integrity of software updates by verifying their digital signatures prior to installation. Various software and cryptographic self-tests are performed at start-up to ensure the secure and correct operation of the TOE. All keying material used for storage encryption is securely generated and protected from disclosure.

4.4. Cryptographic Support

The TOE performs cryptographic operations, which are tested via relevant Cryptographic Algorithm Validation Program (CAVP) certificates. Secure destruction of cryptographic keys and keying material is implemented and occurs during transition to a compliant power saving state, or when the key or keying material is no longer needed.

5. Assumptions and Clarification of Scope

5.1. Assumptions

The Security Problem Definition, including the assumptions, can be found in the following document:

- *collaborative Protection Profile for Full Drive Encryption - Authorization Acquisition*, Version 2.0 + Errata 20190201, February 1, 2019
- *collaborative Protection Profile for Full Drive Encryption - Encryption Engine*, Version 2.0 + Errata 20190201, February 1, 2019

That information has not been reproduced here. CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E should be consulted if there is interest in that material.

5.2. Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made in accordance with the assurance activities specified in CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E and performed by the Evaluation team.
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication, and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6. Documentation

The following guidance documents are provided with the TOE upon delivery in accordance with the PP:

- *KLC Group LLC CipherDriveOne Kryptr 1.1.0 Common Criteria Guide*, Version 1.1, April 2024
- *KLC Group LLC CipherDriveOne Kryptr Administrator Guide*, V 1.0.1, 4-18-2024

All documentation delivered with the product is relevant to and within the scope of the TOE. This document is the only documentation that should be trusted to set-up, administer, or use the product in the evaluated configuration. Additional documentation was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

7. IT Product Testing

This section describes the testing efforts of the Evaluation team. It is derived from information contained in *KLC Group CipherDriveOne Kryptr 1.1.0 Assurance Activity Report,* Version 0.3, April 2024 (AAR). The AAR provides an overview of testing and the prescribed evaluation activities.

7.1. Developer Testing

No evidence of developer testing is required in the SARs or Evaluation Activities.

7.2. Evaluation Team Independent Testing

The Evaluation team conducted independent testing at Lightship Security USA in Baltimore, MD from September 2023 until April 2024. The Evaluation team configured the TOE according to vendor installation instructions and as identified in the Security Target.

The Evaluation team confirmed the technical accuracy of the setup and installation guide during installation of the TOE. The Evaluation team confirmed that the TOE version delivered for testing was identical to the version identified in the ST.

The Evaluation team used the Protection Profile test procedures as a basis for creating each of the independent tests as required by the Evaluation Activities.

Each Evaluation Activity was tested as required by the conformant Protection Profile and the evaluation team verified that each test passed.

7.3. TOE Test Environment Configuration

The TOE testing environment components are identified in Figure 1 below.

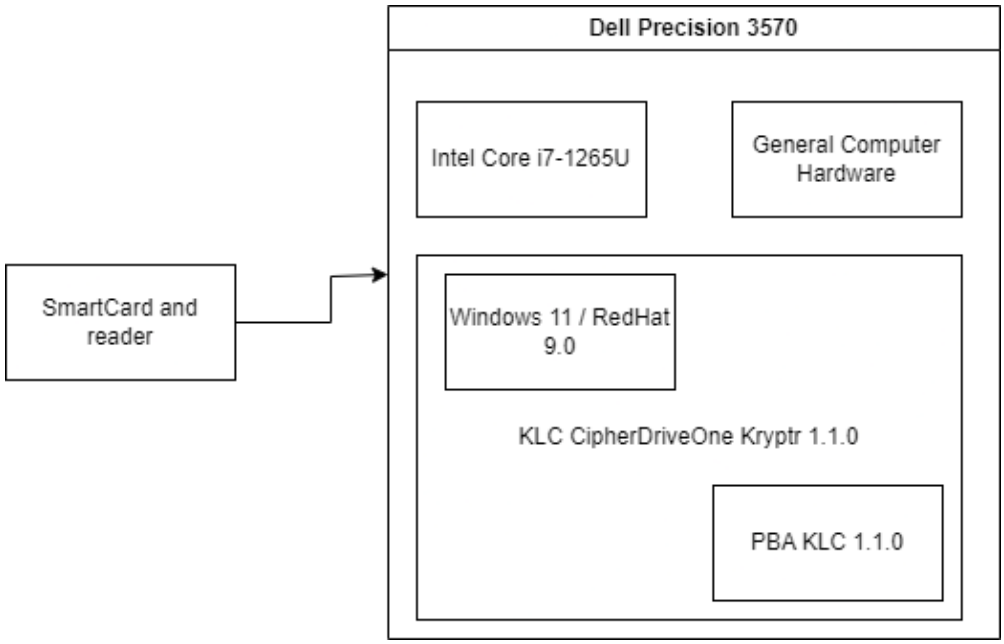

Figure 1: Testing Environment Overview

8. Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that all activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC Version 3.1 Revision 5 and CEM Version 3.1 Revision 5. The evaluation determined KLC Group LLC CipherDriveOne Kryptr 1.1.0 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Evaluation Activities specified in CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E and their supporting documents.

8.1. Evaluation of Security Target (ASE)

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the KLC Group LLC CipherDriveOne Kryptr 1.1.0 that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.2. Evaluation of Development Documentation (ADV)

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST and Guidance documents. Additionally, the Evaluation team performed the Evaluation Activities related to the examination of the information contained in the TOE Summary Specification (TSS).

The Validation reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.3. Evaluation of Guidance Documents (AGD)

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.4. Evaluation of Life Cycle Support Activities (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was appropriately labeled with a unique identifier consistent with the TOE identification in the evaluation evidence and that the TOE references used are consistent.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.5. Evaluation of Test Documentation and the Test Activity (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Test Evaluation Activities in the CPP_FDE_AA_V2.0E and CPP_FDE_EE_V2.0E and recorded the results in the DTR, summarized in the AAR.

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.6. Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the *KLC Group LLC CipherDriveOne Kryptr 1.1.0 Vulnerability Assessment*, Version .2, April 2024, report prepared by the Evaluation team. The vulnerability analysis includes a public search for vulnerabilities. The public search for vulnerabilities conducted on April 17, 2024, did not uncover any residual vulnerability.

The Evaluation team searched:

- NIST National Vulnerabilities Database (can be used to access CVE and US-CERT databases identified below): https://web.nvd.nist.gov/view/vuln/search
- Common Vulnerabilities and Exposures: https://cve.mitre.org/cve/search_cve_list.html
- US-CERT: http://www.kb.cert.org/vuls/html/search

The Evaluation team performed a search using the following keywords:

- KLC CipherDriveOne Kryptr
- CipherDriveOne Kryptr
- CipherDriveOne
- Kryptr
- Drive Encryption

- Disk Encryption
- Key destruction
- Key sanitization
- Opal management software
- SED management software
- Password caching
- Key caching
- BoringSSL
- OpenSSL fips object module
- Libgcrypt
- Cryptsetup
- OpenSSL
- Opensc
- Windows CryptoAPI
- Linux Crypto API
- Linux Kernel 5.15

The Validation team reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

8.7. Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team followed the procedures defined in the CEM and performed the Evaluation Activities in CPP_FDE_AA_V2.0E, CPP_FDE_EE_V2.0E, and their supporting documents and correctly verified that the product meets the claims in the ST.

9. Validator Comments

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the documentation referenced in Section 6 of this VR. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness. No versions of the TOE and software, either earlier or later, were evaluated.

10. Annexes

Not applicable.

11. Security Target

KLC Group LLC CipherDriveOne Kryptr 1.1.0 Security Target, Version 1.5, April 2024

12. GLOSSARY

- **Common Criteria Testing Laboratory (CCTL):** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance:** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation:** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence:** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature:** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE):** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Threat:** Means through which the ability or intent of a threat agent to adversely affect the primary functionality of the TOE, facility that contains the TOE, or malicious operation directed towards the TOE. A potential violation of security.
- **Validation:** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body:** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.
- **Vulnerabilities:** A vulnerability is a hardware, firmware, or software flaw that leaves an Automated Information System (AIS) open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, which could be exploited by a threat to gain unauthorized access to information or disrupt critical processing.

13. Acronym List

CAVP	Cryptographic Algorithm Validation Program (CAVP)
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCTL	Common Criteria Testing Laboratories
CEM	Common Evaluation Methodology for IT Security Evaluation
LS	Lightship Security USA CCTL
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OSP	Organizational Security Policies
PCL	Products Compliant List
ST	Security Target
TOE	Target of Evaluation
VR	Validation Report

14. Bibliography

1. *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2017-04-001*, Version 3.1 Revision 5, April 2017
2. *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2017-04-002*, Version 3.1 Revision 5, April 2017
3. *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2017-04-003*, Version 3.1 Revision 5, April 2017
4. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2017-04-004*, Version 3.1, Revision 5, April 2017
5. *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, v2.0 + Errata 20190201,* February 1, 2019
6. *collaborative Protection Profile for Full Drive Encryption – Encryption Engine, v2.0 + Errata 20190201,* February 1, 2019
7. *KLC Group LLC CipherDriveOne Kryptr 1.1.0 Common Criteria Guide,* Version 1.1, April 2024
8. *KLC Group LLC CipherDriveOne Kryptr Administrator Guide V 1.0.1, 4-18-2024*
9. *KLC Group LLC CipherDriveOne Kryptr 1.1.0 Security Target,* Version 1.5, April 2024
10. *KLC Group CipherDriveOne Kryptr 1.1.0 Key Management Description,* Version 1.4, April 2024
11. *KLC Group CipherDriveOne Kryptr 1.1.0 Assurance Activity Report,* Version 0.3, April 2024
12. *KLC Group LLC CipherDriveOne Kryptr 1.1.0 Vulnerability Assessment,* Version 0.2, April 2024
13. *KLC Group CipherDriveOne Kryptr 1.1.0 Evaluation Technical Report,* Version 0.3, April 2024
14. *KLC Group LLC CipherDriveOne Kryptr 1.1.0 cPP FDE AA+EE 2.0E Test Plan,* Version 0.4, April 2024
15. *KLC Group LLC CIpherDriveOne Kryptr 1.1.0 cPP FDE AA+EE 2.0E Test Evidence,* Version 0.4, April 2024